



NATIONAL SECURITY AGENCY
INFORMATION ASSURANCE DIRECTORATE

**Commercial Solutions for Classified (CSfC)
Virtual Private Network (VPN)
Capability Package**

Version 1.08
March 04, 2013

CHANGE HISTORY

Title	Version	Date	Change Description
Commercial Solutions for Classified (CSFC) Site-to-Site Virtual Private Network (S2S VPN) Capability Package	0.8	February 8, 2012	<ul style="list-style-type: none"> Initial release of CSfC Virtual Private Network (VPN) guidance.
Commercial Solutions for Classified (CSFC) Multi-Site Virtual Private Network Capability Package	1.0	August 17, 2012	<ul style="list-style-type: none"> Official release of CSfC VPN guidance. Adjudicated public review of Site-to-Site VPN CP. Document title changed to reflect approved possible network configurations.
Commercial Solutions for Classified (CSfC) Virtual Private Network Capability Package	1.08	March 4, 2013	<ul style="list-style-type: none"> Initial release of CSfC VPN guidance for remote access. Added Remote Access Architecture and associated requirements and test procedures. Split compound requirements into separate requirements. Assigned requirement identifiers to “shall” statements in Sections 4 and 5 of Multi-Site VPN CP 1.0. Explicitly identified which requirements apply to each architecture. Explicitly identified threshold and objective requirements.

TABLE OF CONTENTS

1. INTRODUCTION.....	1
2. PURPOSE OF THIS DOCUMENT	1
3. USE OF THIS DOCUMENT	2
4. DESCRIPTION OF THE VPN SOLUTIONS	3
4.1 INTEROPERABILITY	5
4.2 ARCHITECTURE	6
4.2.1 ARCHITECTURE FOR MULTIPLE INDEPENDENT SITES	6
4.2.2 ARCHITECTURE WITH A CENTRAL MANAGEMENT SITE.....	7
4.2.3 ARCHITECTURE WITH REMOTE ACCESS.....	9
4.2.4 COMBINING ARCHITECTURES.....	11
5. SOLUTION COMPONENTS.....	11
5.1 OUTER VPN GATEWAY	12
5.2 INNER VPN GATEWAY.....	12
5.3 CERTIFICATE AUTHORITIES	13
5.4 ADMINISTRATION DEVICES	13
5.5 END USER DEVICE.....	14
5.5.1 INNER VPN CLIENT.....	14
5.5.2 OUTER VPN CLIENT	15
5.6 OTHER CONTROLS	15
6. KEY MANAGEMENT.....	15
7. OVERALL SYSTEM SECURITY.....	17
7.1 PASSIVE THREATS	17
7.2 EXTERNAL (ACTIVE) THREATS	18
7.2.1 ROGUE TRAFFIC	18
7.2.2 MALWARE AND UNTRUSTED UPDATES	19
7.2.3 DENIAL OF SERVICE	19
7.2.4 SOCIAL ENGINEERING	19
7.3 INSIDER THREATS	19
7.4 SUPPLY CHAIN THREATS	20
7.5 INTEGRATOR THREATS	21
7.6 ADDITIONAL MITIGATION INFORMATION	21
8. VPN SOLUTION ARCHITECTURE AND CONFIGURATION REQUIREMENTS...	22
9. GUIDELINES FOR SELECTING COMPONENT PRODUCTS	22
10. CONFIGURATION.....	24
10.1 OVERALL SOLUTION REQUIREMENTS.....	24
10.2 CONFIGURATION REQUIREMENTS FOR ALL VPN COMPONENTS	25

10.3 ADDITIONAL REQUIREMENTS FOR INNER VPN COMPONENTS	27
10.4 ADDITIONAL REQUIREMENTS FOR OUTER VPN COMPONENTS	27
10.5 REQUIREMENTS FOR END USER DEVICES	28
10.6 PORT FILTERING REQUIREMENTS FOR VPN COMPONENTS	30
10.7 CONFIGURATION CHANGE DETECTION REQUIREMENTS	31
10.8 REQUIREMENTS FOR VPN COMPONENT ADMINISTRATION.....	31
10.9 AUDITING REQUIREMENTS	32
10.10 KEY MANAGEMENT REQUIREMENTS	33
10.10.1 PKI REQUIREMENTS FOR VPN COMPONENTS.....	33
10.10.2 ENTERPRISE PKI REQUIREMENTS.....	34
10.10.3 LOCALLY-RUN PKI REQUIREMENTS.....	34
11. GUIDANCE FOR THE USE AND HANDLING OF SOLUTIONS.....	35
12. ROLE-BASED PERSONNEL REQUIREMENTS	37
13. INFORMATION TO SUPPORT AO/DAA.....	39
13.1 SOLUTION TESTING	39
13.2 RISK ASSESSMENT.....	41
13.3 REGISTRATION OF SOLUTIONS	41
14. TESTING REQUIREMENTS.....	41
14.1 PRODUCT SELECTION	41
14.2 PHYSICAL LAYOUT OF SOLUTION	42
14.3 END USER DEVICE CONFIGURATIONS.....	43
14.4 VPN COMPONENT CONFIGURATIONS	44
14.5 CA CONFIGURATIONS.....	45
14.6 VPN GATEWAY ADMINISTRATION.....	46
14.7 SOLUTION FUNCTIONALITY	47
14.8 APPROPRIATE PACKETS TRAVERSING THE SOLUTION.....	47
14.9 APPROPRIATE PACKETS TRANSFERRING THE EUD	49
14.10 SECURITY ASSOCIATION LIFETIMES	50
14.11 USE OF CERTIFICATES FROM UNTRUSTED CAS.....	50
14.12 USE OF REVOKED CERTIFICATES	51
14.13 CONFIGURATION CHANGE DETECTION	52
14.14 AUDIT.....	53
14.15 IMPLEMENTATION OF GUIDANCE	54
APPENDIX A. GLOSSARY OF TERMS	56
APPENDIX B. ACRONYMS.....	59
APPENDIX C. REFERENCES	61
APPENDIX D. EXAMPLE IAD APPROVAL LETTER FOR VPN CAPABILITY	

PACKAGE SOLUTIONS	64
APPENDIX E. END USER DEVICE IMPLEMENTATION NOTES.....	65
EXAMPLE EUD IMPLEMENTATION APPROACHES	65
EXAMPLE 1: TYPE 2 VIRTUALIZATION.....	65
EXAMPLE 2: TYPE 1 VIRTUALIZATION.....	67
EXAMPLE 3: EXTERNAL OUTER IPSEC CLIENT DEVICE	68
UML SEQUENCE DIAGRAM FOR EUD TUNNEL ESTABLISHMENT	69

TABLE OF FIGURES

Figure 1. Two IPsec Tunnels Protect Data across a Black Network	4
Figure 2. Two IPsec Tunnels Provide Remote Access across a Black Network	5
Figure 3. VPN Architecture for Multiple Independent Sites	7
Figure 4. VPN Architecture with a Central Management Site	8
Figure 5. VPN Architecture with Remote Access	10
Figure 6. Example EUD Implementation using Type 2 Virtualization	66
Figure 7. Example EUD Implementation using Type 1 Virtualization	67
Figure 8. Example EUD Implementation using an External Outer IPsec Client Device	68

LIST OF TABLES

Table 1. Product Selection Requirements	23
Table 2. CSfC Component Lists for the VPN Products.....	23
Table 3. Overall Solution Requirements.....	24
Table 4. Approved Suite B Algorithms	25
Table 5. Configuration Requirements for Both VPN Components	25
Table 6. Additional Requirements for Inner VPN Components.....	27
Table 7. Additional Requirements for Outer VPN Components	27
Table 8. Requirements for End User Devices.....	28
Table 9. Port Filtering Requirements for VPN Components.....	30
Table 10. Configuration Change Detection Requirements	31
Table 11. Requirements for VPN Component Administration.....	31
Table 12. Auditing Requirements	32
Table 13. PKI Requirements for VPN Components.....	33
Table 14. Enterprise PKI Requirements	34
Table 15. Locally-Run PKI Requirements.....	34
Table 16. Guidance for the Use and Handling of Solutions	35
Table 17. Role-Based Personnel Requirements.....	38
Table 18. Test Requirements	40

1. INTRODUCTION

The Commercial Solutions for Classified (CSfC) program within the National Security Agency (NSA) Information Assurance Directorate (IAD) uses a series of Capability Packages to provide configurations that will allow customers to independently implement secure solutions using layered Commercial Off-the-Shelf (COTS) products. The Capability Packages are vendor-agnostic and provide high level security and configuration guidance for customers and/or Solution Integrators.

IAD is delivering a generic CSfC Virtual Private Network (VPN) Capability Package to meet the demand for data in transit solutions using a secure sharing suite (S3) of algorithms [NSA Suite B]. These algorithms, known as Suite B algorithms, are used to protect classified data using layers of COTS products. VPN Capability Package Version 1.08 enables customers to implement VPNs for connectivity between two or more sites, VPNs for remote access by End User Devices, or both. This Capability Package takes lessons learned from four proof-of-concept demonstrations that had implemented a set of S3 algorithms, modes of operation, standards, and protocols. These demonstrations included a layered use of COTS products for the protection of classified information.

This initial version of the CSfC VPN Capability Package does **not** supersede the CSfC Multi-Site VPN Capability Package Version 1.0 dated 17 August 2012. The final version of this Capability Package, expected to be released as Version 2.0, is intended to supersede the CSfC Multi-Site VPN Capability Package. Until the release of Version 2.0, the CSfC Multi-Site VPN Capability Package Version 1.0 dated 17 August 2012 is the Capability Package to be used for implementing a CSfC Multi-Site VPN solution.

2. PURPOSE OF THIS DOCUMENT

This Capability Package provides reference architectures and corresponding configuration information that would allow customers to select COTS products from the CSfC Components List for their VPN solution and then to properly configure those products to achieve a level of assurance sufficient for protecting classified data while in transit. As described in Section **Error! Reference source not found.** customers must ensure that the components selected from the CSfC Components List will permit the necessary functionality for the selected architecture. Throughout this document, requirements imposed on the VPN solution, to ensure proper implementation, are notated by a two-letter and number label (e.g., KM11). In addition to the two-letter and number label, requirements imposed on the solution are denoted by the architecture selected by the customer for implementation. To successfully implement a solution based on this Capability Package, all requirements for the selected architecture must be implemented as designated by the “Architecture” column in the requirement tables.

Customers who want to use a variant of the solutions detailed in this Capability Package must contact NSA to determine ways to obtain NSA approval. Additional information about the CSfC process will be available on the CSfC web page (www.nsa.gov/ia/programs/csfc_program).

3. USE OF THIS DOCUMENT

At this time, this document may not be used for a CSfC solution without formally obtaining support from NSA for the effort prior to presenting a solution to the implementing organization's Authorizing Official (AO). United States Government entities interested in presenting solutions to their AOs in accordance with this guidance must first obtain NSA support by submitting a request for Capability Package application support to their NSA/IAD Client Advocate. In the future, however, customers and their solution providers will be able to use this guidance to implement solutions without such NSA/IAD involvement.

Solutions designed according to this Capability Package must be registered with NSA/IAD. Once registered, a signed IAD Approval Letter (see sample in Appendix D) will be sent validating that this VPN Capability Package represents a CSfC solution approved for protecting classified information. Any solution designed according to this Capability Package may be used for one year and must then be revalidated against the current version of the Capability Package.

Please provide comments on usability, applicability, and/or shortcomings to your NSA/IAD Client Advocate and the VPN Capability Package maintenance team at vpn@nsa.gov.

The following Legal Disclaimer relates to the use of this Capability Package:

This Capability Package is provided "as is." Any express or implied warranties, including but not limited to, the implied warranties of merchantability and fitness for a particular purpose are disclaimed. In no event shall the United States Government be liable for any direct, indirect, incidental, special, exemplary or consequential damages (including, but not limited to, procurement of substitute goods or services, loss of use, data, or profits, or business interruption) however caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of this Capability Package, even if advised of the possibility of such damage.

The User of this Capability Package agrees to hold harmless and indemnify the United States Government, its agents and employees from every claim or liability (whether in tort or in contract), including attorney's fees, court costs, and expenses, arising in direct consequence of Recipient's use of the item, including, but not limited to, claims or liabilities made for injury to or death of personnel of User or third parties, damage to or destruction of property of User or third parties, and infringement or other violations of intellectual property or technical data rights.

Nothing in this Capability Package is intended to constitute an endorsement, explicit or implied, by the U.S. Government of any particular manufacturer's product or service.

4. DESCRIPTION OF THE VPN SOLUTIONS

This Capability Package describes two general types of VPN solutions to protect classified information as it travels across either an untrusted network or a network of a different classification level. The first is a VPN between two network enclaves at the same classification level, as shown in Figure 1. The second is a remote-access solution that provides a VPN between a network enclave and an End User Device (EUD) connected directly to the untrusted network outside of that enclave, as shown in Figure 2. A system compliant with this Capability Package may implement either type of VPN solution, or may implement both.

Both types of VPN solutions use two independent Internet Protocol Security (IPsec) tunnels to protect traffic as it transits the untrusted network. For each network enclave in the solution, such as Site A and Site B in Figure 1 or Site A in Figure 2, there is a pair of VPN Gateways between the enclave and the untrusted network. Each VPN Gateway in the pair generates one of the two IPsec tunnels. The VPN Gateways closest to a trusted enclave are referred to as the Inner VPN Gateways. Likewise, the VPN Gateways closest to the untrusted network (i.e., farthest from a trusted enclave) are referred to as the Outer VPN Gateways.

There are no VPN Gateways associated with the EUDs in the remote-access solution, since they connect directly to the untrusted network instead of residing in a trusted enclave. Instead, the EUD itself hosts a pair of VPN Clients, each of which generates one of the two IPsec tunnels on the EUD. The VPN Client on an EUD which establishes an IPsec tunnel with the Outer VPN Gateway for an enclave is referred to as the Outer VPN Client. Likewise, the VPN Client on an EUD which establishes an IPsec tunnel with the Inner VPN Gateway for an enclave is referred to as the Inner VPN Client. (Appendix E provides more details about how this routing within the EUD could be accomplished.) Because they are expected to be used in physical locations where storage of classified material is not available, EUDs are considered to be unclassified while not in use. To prevent classified data from being stored on the EUD, the EUD does not have direct access to the classified enclave through the VPN. Instead, it has access to a Thin Client system on the classified network; the Thin Client application on the EUD allows classified data to be displayed but prevents it from being stored on the EUD.

Throughout this Capability Package, the term “VPN Component” is used to refer generically to VPN Gateways and VPN Clients alike, in situations where the differences between the two are unimportant.

This Capability Package imposes no limit on the number of enclaves that may be interconnected, or on the number of EUDs that may connect to an enclave. An EUD may be used to connect to more than one enclave, as long as it only connects to a single enclave at a time, and all of those enclaves are at the same classification level. The customer is responsible for determining which enclaves will interconnect via VPN, and which enclaves each EUD is authorized to connect to.

The following terms are used throughout this document:

- Red network – the network behind the Inner VPN Gateway.
- Gray network – the network between the Inner and Outer VPN Gateways. This is divided into two sub-networks, as follows:
 - Gray management network – the part of the Gray network that contains the management functions to run the Outer layer, including the Outer tunnel CA and the Outer VPN Gateway admin/audit server functions.
 - Gray data network – the part of the Gray network that sends data between the Inner and Outer VPN Gateways.
- Black network – the network connecting the Outer VPN Gateways.

Figure 1 shows data as it traverses the network from one enclave to another without a remote access capability. Red data exists in the network behind the Inner VPN Gateway; this data is encrypted by the Inner VPN Gateway and sent to the Outer VPN Gateway (this tunnel is depicted in gray). That encrypted data is then encrypted once again, this time by the Outer VPN Gateway and sent across the Black network (the second tunnel shown in black). This ensures that classified information is protected with two layers of encryption as it travels over the Black network, each layer providing both confidentiality and integrity for the data. The reverse process occurs at the other site to fully decrypt the data and pass it to the other Red network.

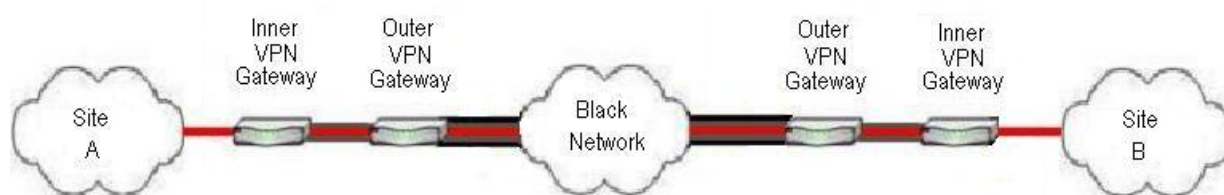


Figure 1. Two IPsec Tunnels Protect Data across a Black Network

Figure 2 similarly shows data as it traverses the network for the remote access solution between an enclave and an EUD. Red data leaving the enclave is encrypted the same way as in the enclave-to-enclave case. When the EUD receives the doubly-encrypted data, it decrypts it first using the Outer VPN Client, and then with the Inner VPN Client, before processing it. Likewise, when the EUD sends data, it first encrypts it with the Inner VPN Client, and then with the Outer VPN Client, before sending it across the Black network. Because of the use of a Thin Client system, the data sent from the enclave to the EUD will primarily consist of content to display on screen, and the data sent from the EUD to the enclave will primarily consist of keyboard and mouse input. If the EUDs are being remotely administered, the data sent from the enclave to the

EUD may also include updates for the software and configuration on the EUD; since these updates are stored on the EUD, they need to be unclassified in their entirety.

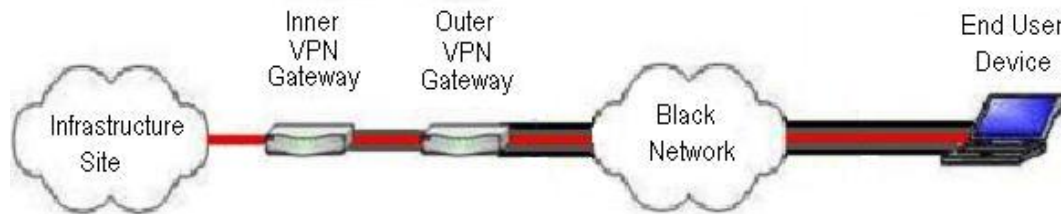


Figure 2. Two IPsec Tunnels Provide Remote Access across a Black Network

The solution for connecting two or more enclaves together provides mutual device authentication during tunnel setup, but does not provide any end user authentication for traffic going through the tunnels. In that solution, any required end user authentication between two sites must be provided separately and will not be considered as a part of this solution.

The solution for remote access between an enclave and an EUD also provides mutual device authentication during tunnel setup. However, it also requires the user of the EUD to authenticate to a Thin Client Server before gaining access to any classified data from it. Because the EUD may be connecting from a physical location other than a secure facility, it is necessary to verify that the person accessing the EUD is authorized to access classified data.

Throughout this document, when IP traffic is discussed, it can either be IPv4 or IPv6, unless otherwise specified. In addition, the Red, Gray and Black networks can run either version and each network is independent from the others in making that decision. In the remainder of the document, if no protocols or standards are specified, then any appropriate protocols may be used to achieve the objective.

Public standards conformant Layer 2 control protocols such as ARP are allowed as necessary to ensure the operational usability of the network. This Capability Package is agnostic with respect to Layer 2; specifically it does not require Ethernet. Public standards conformant Layer 3 control protocols such as ICMP may be allowed based on local AO/DAA policy, but the default configuration of this solution is for all Layer 3 control protocols to be disabled. Red and Gray network multicast messages and IGMP or MLD may also be allowed depending on local AO/DAA policy. Multicast messages received on external interfaces of the Outer VPN component shall be dropped and may be logged.

4.1 INTEROPERABILITY

The solutions defined in this Capability Package support interoperability between different sites, and between sites and EUDs by having similar standards-based configurations at both ends of

each layer of the solution. There is no guarantee of generic interoperability between any two products listed on the CSfC Components List. It is an IAD goal to create and realize adoption of IPsec implementation standards that will allow for this generic interoperability in the future.

4.2 ARCHITECTURE

There are three main architectures that are supported by this Capability Package. Two of them, the architecture for Multiple Independent Sites and the architecture with a Central Management Site, provide a solution for connecting enclaves at two or more sites via a VPN. The third, the architecture for Remote Access, provides a solution for connecting one or more EUDs back to a site via a VPN. A system complying with this Capability Package may implement one, two, or all three of these architectures. Fundamentally, all the VPN solution architectures consists of two IPsec VPN components at each site or EUD that respectively generate the Inner and Outer IPsec tunnels, providing two independent layers of encryption between the sites (see Figure 1 and Figure 2).

Fundamental network architecture components, such as DNS and NTP, are not shown in the figures or explicitly discussed in this document. These components should be located on the inside network of an infrastructure site (the Gray network for Outer VPN Components and the Red network for the Inner VPN Components), except in the case of remote access where basic services on the Black network such as DHCP and DNS may be necessary for an EUD to join the Black network and establish a connection to an Outer VPN Gateway.

It is expected that this solution can be implemented in such a way as to take advantage of standards based routing protocols that are already being used in the network. For example, networks that currently use GRE or OSPF protocols can continue to use these in conjunction with this solution to provide routing, provided that the AO/DAA approves their use.

4.2.1 ARCHITECTURE FOR MULTIPLE INDEPENDENT SITES

In the architecture with multiple independent sites, each site performs the administration of its own VPN Gateways and has the option of using either Certificate Authorities (CAs) that they control (see Figure 3) or, if available, an enterprise CA. Each site needs to ensure that the VPN Gateways it selected interoperate with those at the other sites. In addition, the two VPN Gateways at each site need to have the signing certificate and revocation information for the corresponding CAs used by the other sites in the system installed. The Gray Management and Gray Data networks are physically separate from one another at each site, and no management traffic crosses the Black network, encrypted or otherwise.

This architecture requires cooperation between the various sites in the solution to ensure that all CAs used by each site are trusted at all the other sites. This model has the advantage of allowing communication between larger organizations that have a need to share information while maintaining independence.

Note that while Figure 3 depicts two independent sites, this solution can scale to include numerous sites with each additional site having the same architecture as Site B.

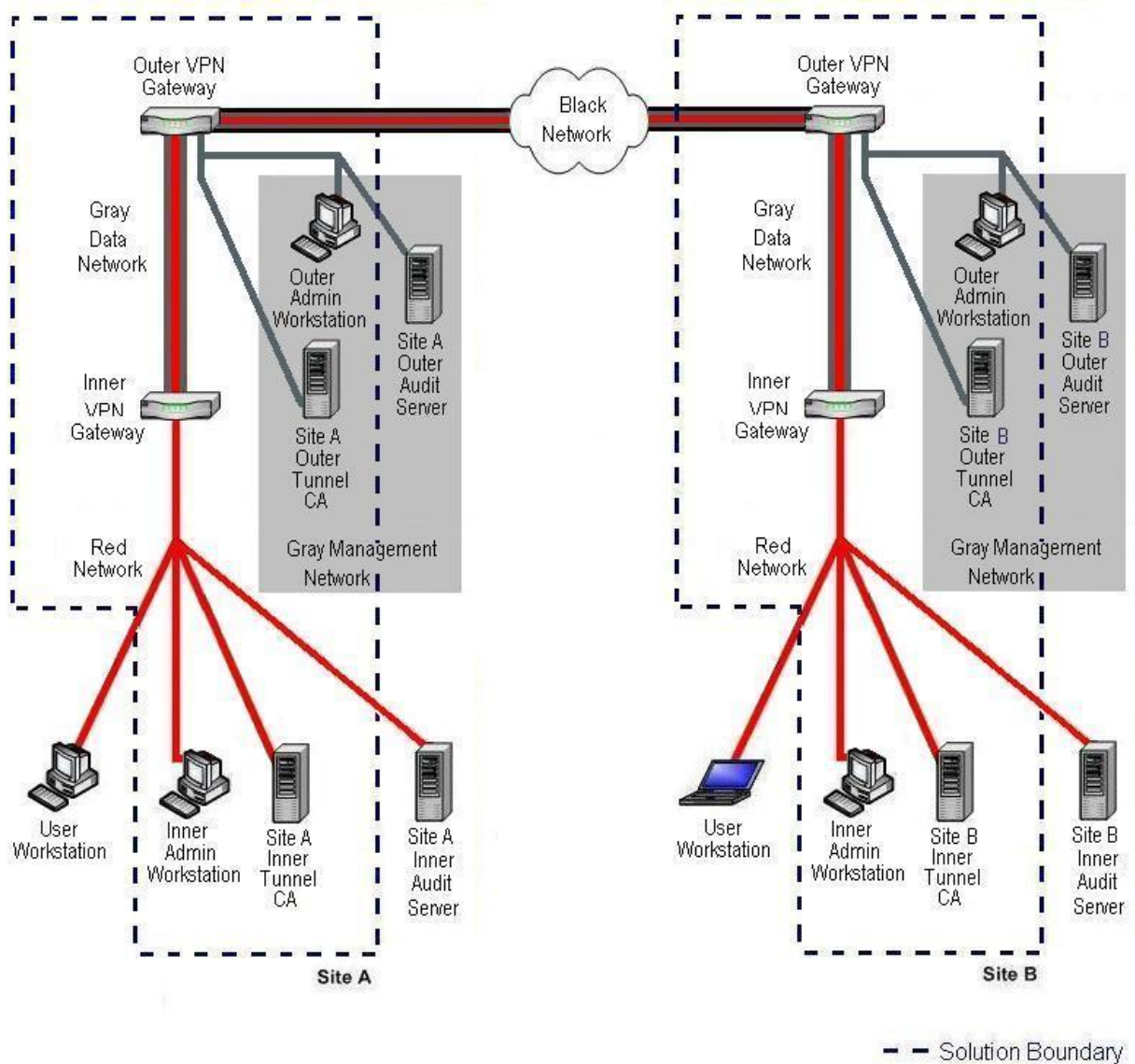


Figure 3. VPN Architecture for Multiple Independent Sites

4.2.2 ARCHITECTURE WITH A CENTRAL MANAGEMENT SITE

In the architecture with a central management site, a single site administers and performs keying for all the various sites included in the solution. Figure 4 provides an example of this architecture, where Site A is the central management site and Site B is one of potentially many other sites in the network. In this case, because the administration is done by one group of Security Administrators and CA Administrators (see Section 12), they can ensure interoperability of each site as new sites are added. Only two CAs are needed: one on the Red network for all the

Inner VPN Gateways and one on the Gray management network for all the Outer VPN Gateways. If available, enterprise CAs may be used.

Because the central management site manages the VPN Gateways at the other sites over the network, encryption is used to separate data and management traffic as it passes between sites. Gray management traffic is encrypted using SSH, TLS, or IPsec before being routed through the Outer VPN Gateway to another site. Red management traffic is similarly encrypted before being routed through the Inner and Outer VPN Gateways to another site.

This model makes it easier to add sites because of the centralized administration.

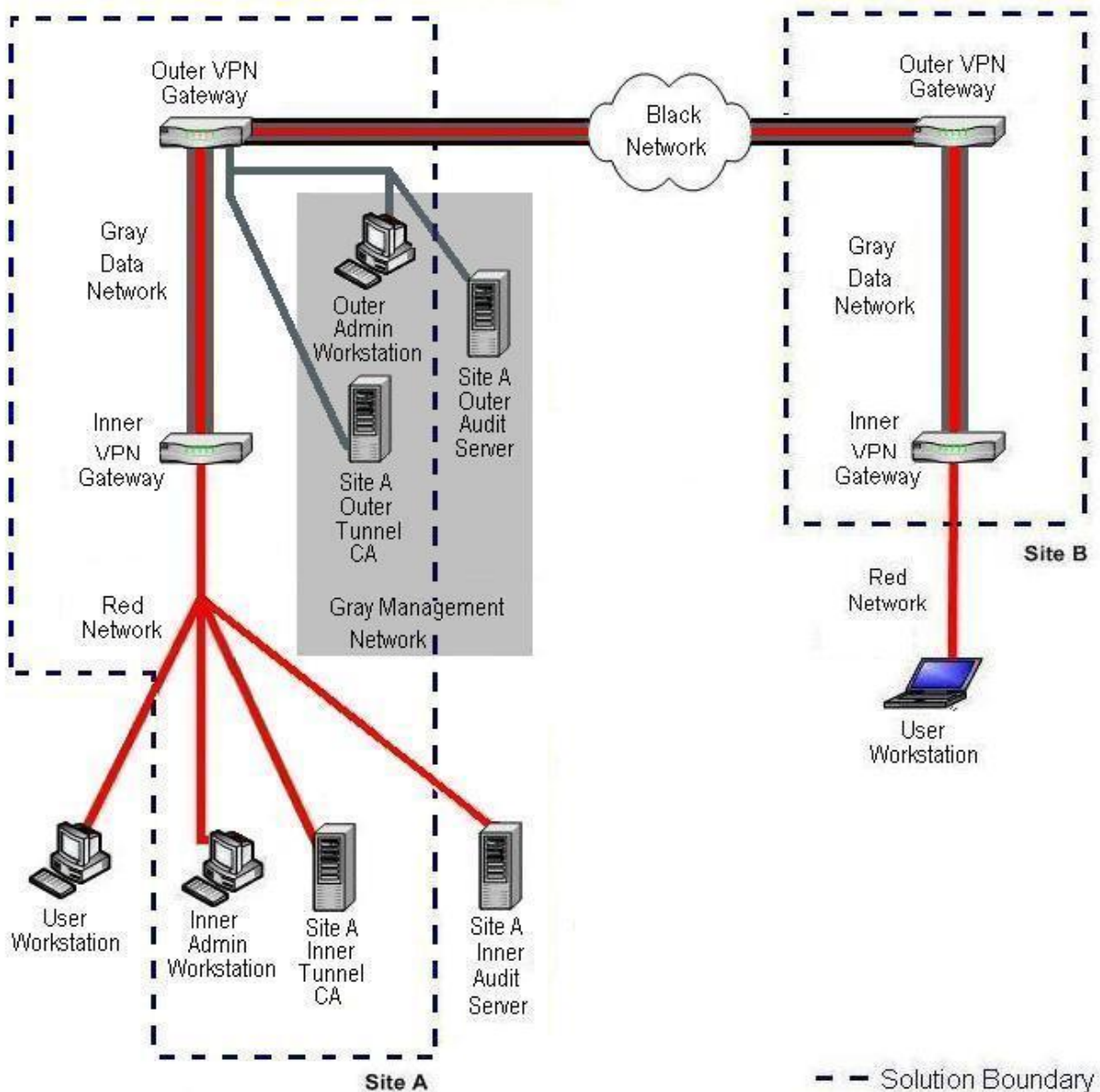


Figure 4. VPN Architecture with a Central Management Site

Note that while Figure 4 depicts two sites, this solution can scale to include numerous sites, with each additional site having the same architecture as Site B.

4.2.3 ARCHITECTURE WITH REMOTE ACCESS

In the architecture with remote access, a single infrastructure site administers and performs keying for all the various EUDs included in the solution. Figure 5 provides an example of this architecture, where the infrastructure site is on the left and one of potentially many EUDs in the solution is on the right. Because the administration is done by one group of Security Administrators and CA Administrators (see Section 12), they can ensure interoperability of each EUD in the solution. Only two CAs are needed: one on the Red network for all the Inner VPN Components and one on the Gray management network for all the Outer VPN Components. If available, enterprise CAs may be used.

The EUD is only treated as a classified device while in use and when disposed of. At all other times, although the EUD is still physically protected to prevent access by unauthorized persons, it is considered an unclassified device. This allows the EUD to provide classified network access to travelers, teleworkers, continuity-of-operations personnel, and other cleared and authorized users without physical access to a classified network enclave. The organization implementing the remote-access system is responsible for establishing terms of use for its EUDs, to protect classified information displayed on the EUD from disclosure.

EUDs may be remotely administered through the VPN solution. Remote administration of the Outer VPN Client is performed from the Gray Management network of the infrastructure site. Remote administration of the Inner VPN Client and Thin Client Application are performed from the Red network of the infrastructure site.

The VPN Gateways used in the remote access architecture will need to implement VPN head-end functionality required by the VPN Clients on the EUDs, which enables the VPN Gateways to assign IP addresses, manage client sessions, and perform other management functions for the VPN Clients.

To allow the EUD to be treated as unclassified when not in use, data from the Red network must not be stored on the EUD. To enforce this, the EUD can only access the Red network through a Thin Client system, instead of having direct access into a Red network enclave through the VPN as is done in the other two architectures. The Thin Client Application on the EUD is configured to prohibit classified data from the Red network from being stored persistently on the EUD. (If the EUD is remotely managed, updated software and configuration data may be written to the EUD, but such updates are not distributed through the Thin Client connection.) To prevent a lost or stolen EUD from being used by an unauthorized person to access the classified network, the user authenticates to the Thin Client Server before being granted access.

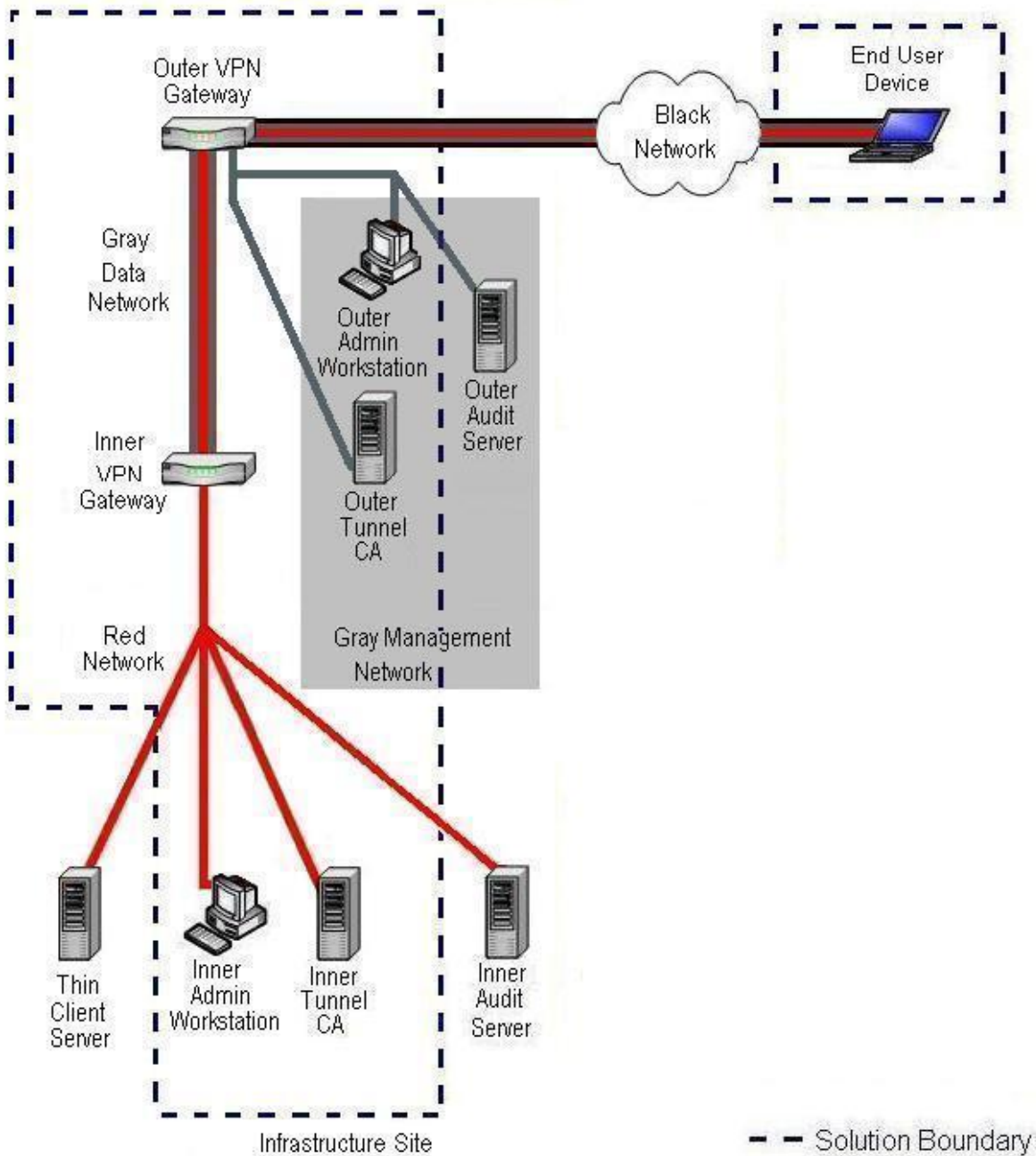


Figure 5. VPN Architecture with Remote Access

Note that while Figure 5 depicts a single EUD, this solution can scale to include numerous End User Devices.

4.2.4 COMBINING ARCHITECTURES

A solution compliant with this Capability Package may implement more than one of the above architectures together, as long as the solution meets all of the requirements for each architecture implemented.

For example, suppose Organization A has multiple physical sites it wishes to interconnect via VPN, and also has a need to securely communicate with Organization B. Organization A can implement the Central Management Site architecture across each of its own sites and the Multiple Independent Sites architecture for its interconnection with Organization B.

Organization A's central site only needs to deploy a single pair of VPN Gateways, which provide VPN connections to Organization B as well as VPN connections to Organization A's other sites. Likewise, the pair of CAs it uses for its interconnection with Organization B can be the same pair of CAs used to generate certificates for each of Organization A's sites.

Similarly, the pair of VPN Gateways at Organization A's central site can double as the infrastructure site that the EUDs of its remote users connect into, assuming that the specific products used as the VPN Gateways implement any VPN head-end functionality needed by the VPN Clients on the EUDs. To comply with the requirements of this Capability Package, the Inner VPN Gateway will need to be configured to restrict EUDs to accessing only the Thin Client Server while allowing connections from VPN Gateways at other sites to access the Red network directly.

5. SOLUTION COMPONENTS

In the architectures discussed in the previous section, there are two IPsec VPN components that exist at each site or within the End User Device. These components generate two IPsec tunnels, which provide two layers of encryption between the sites or between a site and a EUD (see Figure 1 and Figure 2). In addition to the VPN components, mandatory aspects of the solution include administration devices and CAs for key management using Public Key Infrastructure (PKI).

Each component is described below. The descriptions include information about the security provided by the components as evidence for why they are deemed mandatory for the solution. Overall System Security is discussed in Section 7.

Additional components are discussed in Section 5.6 that can be added to the solution to help reduce the overall risk. However, these are not considered mandatory components for the security of the solution and, therefore, will not have configuration or security requirements placed on them.

5.1 OUTER VPN GATEWAY

Authentication of a peer VPN component, cryptographic protection of data in transit, and configuration and enforcement of network packet handling rules are all aspects fundamental to the security provided by a VPN Gateway.

The Outer VPN Gateway located at the edge of the private network generates an IPsec tunnel, which provides device authentication and confidentiality and integrity of information traversing the unsecure/untrusted Black network. VPNs offer a decreased risk of exposure of information in transit since any information that traverses the Black network is placed in a secure tunnel that provides an authenticated and encrypted path between two sites.

Although the Outer VPN Gateway is a perimeter VPN Gateway and thus more exposed to external attacks, the VPN Gateway is also capable of protecting the network from unauthenticated traffic through use of an internal filtering capability. This allows specification of rules that prohibit unauthorized data flow which helps mitigate Denial of Service (DoS) attacks and prevent resource exhaustion. This solution does not require that the Outer VPN Gateway terminate all VPNs on a single physical interface; however, all such external interfaces shall conform to the port filtering requirements in Section 10.6. The Outer VPN Gateway is implemented identically for all the architectures covered in this Capability Package.

There is some data that will originate from the Outer VPN Gateway (such as control traffic (e.g., BFD), logging and audit data, which will potentially be sent to the Gray Management network at another site) that will only go through a single IPsec tunnel. This is the only exception to having two layers of encryption for data going over the Black network and is considered acceptable given the intelligence value of that information.

5.2 INNER VPN GATEWAY

Similar to the Outer VPN Gateway, the Inner VPN Gateway provides authentication of a peer VPN component, cryptographic protection of data in transit, and configuration and enforcement of network packet handling rules. Unlike the Outer VPN Gateway, however, the Inner VPN Gateway is not a perimeter VPN Gateway and, therefore, not as exposed to external attacks, but it is more exposed to an internal attack.

The Inner VPN offers a decreased risk of exposure for data-in-transit by providing an encrypted tunnel between two sites. Along with the Outer VPN, this results in a solution with two layers of IPsec providing protection for the data-in-transit. Any single layer using Suite B algorithms should be strong enough for such a VPN solution. However, a single layer may be prone to vulnerabilities introduced accidentally through implementation or operator error, or intentionally by an adversary leading to compromise of sensitive information. The addition of multiple layers reduces the likelihood that such a vulnerability can be exploited to attack the full solution, particularly if the layers exhibit suitable independence.

If the Outer VPN is compromised or fails in some way, the Inner VPN can still provide the needed security for the data. In addition, the Inner VPN Gateway can indicate that a failure of the Outer VPN Gateway has occurred. Through the use of its internal filtering capability, the Inner VPN Gateway is capable of protecting the network from unknown traffic by logging information about the packets received. This will indicate that the Outer VPN Gateway has been breached or misconfigured to permit traffic to pass through to the Inner VPN Gateway that is not allowed.

When the Remote Access Architecture is used for this Capability Package, the Inner VPN Gateway will act as a head-end device. It will be configured with the appropriate security policy in order to ensure that only traffic related to the Thin Client or remote management is being exchanged with the EUD. The head-end device will be configured to allow only traffic defined by requirement PF1.

5.3 CERTIFICATE AUTHORITIES

The CA issues digital certificates for the VPN Gateways and VPN clients in this solution. These certificates are used for authentication in establishing the IPsec tunnels between the sites. Given the architecture of the solution, there are distinct CAs for the Inner and Outer VPNs. The CA providing certificates for the Inner VPN is located on the Red network, and the CA providing certificates for the Outer VPN is located on the Gray management network. This provides the key management separation required for two independent layers of encryption.

5.4 ADMINISTRATION DEVICES

Each VPN Gateway shall also have an administration platform on the appropriate network that allows for maintaining, monitoring, and controlling all security functionality for the particular VPN Gateway. This administration device shall also allow for logging and configuration management, as well as reviewing audit logs. Given the architecture of the solution, there are distinct administration networks for the Inner and Outer VPN Gateways. The administration devices for the Inner VPN are located on the Red network, and the administration devices for the Outer VPN are located on the Gray management network, which shall not be directly connected to the Black or Red networks. This provides the separation necessary for two independent layers and supports the requirement for separate roles for each site.

In the Remote Access architecture, the Administrative Devices are also responsible for configuring and managing the EUD in accordance with this Capability Package in order to allow for an End User to access enterprise data. The administration devices for the Thin Client Application and Inner VPN Client are located on the Red network, and the administration devices for the Outer VPN Client are located on the Gray management network. The Thin Client Application is configured to prohibit saving files from the Thin Client Server to the EUD (see EU1).

5.5 END USER DEVICE

Within the Remote Access Architecture, an EUD shall be used in order to access enterprise data via a Thin Client system. The EUD will not have local storage capability. The Outer and Inner VPN IPsec tunnels will terminate on the EUD from the Outer VPN device and Inner VPN Device located at the infrastructure site (see Figure 5). In order to accomplish this functionality, there are two VPN clients (an Inner and Outer VPN Client) installed on the EUD. The Inner and Outer VPN Clients come from different vendors. Neither vendor can be a subsidiary of the other (see requirement PS5). The Inner VPN Client acts as an intermediary between the Thin Client Application and the logically separated Outer VPN Client.

The EUD Operating System enforces network packet handling rules in order to achieve interoperability between VPN devices. EUDs are provisioned by Administrative devices located at the infrastructure site. The provisioning process includes assigning identifiers to the EUDs, installing required applications, configuring the device's policy and settings, and loading certificates and keying material (see EU12). The EUD will have separate keys for the Inner and Outer VPN Client. The EUD will have Full Disk Encryption in order to protect the device authentication keys stored on it from disclosure and to protect its software and configuration settings from being tampered with by unauthorized individuals. The EUD shall be configured, maintained, and operated in conformance with requirements in Section 10.5 and Section 12.

Unlike other components within the solution, the EUD is only treated as a classified device while in use or during disposal. At all other times, it is treated as unclassified, although it is still subject to physical protection requirements identified in an organization-defined user agreement.

As previously mentioned, there are two VPN clients on the EUD that provide authentication to the infrastructure site VPN devices and cryptographic protection of data in transit. The Inner and Outer VPN Clients are discussed in the following subsections.

5.5.1 INNER VPN CLIENT

The Inner VPN Client is a component within the EUD. The purpose of the Inner VPN Client is to establish an IPsec tunnel from the EUD to the Inner VPN gateway located in the infrastructure site. The tunnel can be configured to automatically be established as part of the EUD's power-on process, following establishment of the Outer tunnel.

Remote administration is not a requirement of this Capability Package. However, if remote administration is implemented, the Inner VPN Client administration management will be performed over the Red Network. Administrative data from the EUD must be protected as prescribed in this Capability Package. Although the Inner and Outer VPN Clients both run on the same EUD, logical separation is still achieved through the use of separate private key stores and IP stacks for each VPN Client. Appendix E provides example design choices that system

developers can make when implementing their EUDs and illustrates how this separation may be implemented.

5.5.2 OUTER VPN CLIENT

The Outer VPN Client is a component within the EUD. The purpose of the Outer VPN Client is to establish an IPsec tunnel from the EUD to the Outer VPN gateway located in the infrastructure site in order to provide access to the Black network. The tunnel can be configured to automatically be established as part of the EUD's power-on process.

Remote administration is not a requirement of this Capability Package. However, if remote administration is implemented, the Outer VPN Client administration management will be performed over the Gray management network. Administrative data from the EUD must be protected as prescribed in this Capability Package. Although the Inner and Outer VPN Clients both run on the same EUD, logical separation is still achieved through the use of separate private key stores and IP stacks for each VPN Client. Appendix E provides example design choices that system developers can make when implementing their EUDs and illustrates how this separation may be implemented.

5.6 OTHER CONTROLS

There are additional controls that could be used within this solution to potentially reduce the overall risk. First, if the VPN solution attaches directly behind an existing router from a site that connects to the Black network, then from the VPN solution perspective, the existing router is considered part of the Black network infrastructure, though it provides some level of filtering and attack detection for the solution. Second, a more comprehensive Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) could be used if additional assurance is desired. A comprehensive IDS or IPS system could increase the difficulty of a rogue actor performing activities with the networks. However, it should be noted that use of these systems on the Gray data network needs to be dedicated to monitoring that network and not interconnected with an IDS or IPS on the Red (or Black) network. Additionally, security administrators could monitor user connection metrics for anomalies and monitor individual user sessions. All monitoring of user sessions and Thin Client metrics will be conducted from the Red network. Finally, if an integrator is used for implementation of this solution, the customer can require separation of roles between individuals working on Red and Gray components. The separation of roles ensures that during the development of the solution no single individual can compromise Red and Gray components simultaneously.

6. KEY MANAGEMENT

One of the most difficult parts of any solution is determining how the key management will be implemented in a secure manner. In this solution, the only certificates necessary are for the

device authentication certificates on each of the two VPN components at the end of each IPsec tunnel.

No single CA can provide keys to both the Inner and Outer VPN components. The CA for the Outer VPN components shall be located in the Gray management network, connected to an Outer VPN Gateway. Since the Gray management network is a small local network, a Locally-run CA will usually need to be stood up to key the Outer VPN components, requiring that a CA product be selected from the NSA-approved CSfC Component List for the Outer tunnel PKI. In addition, a Certificate Policy (CP)/Certification Practice Statement (CPS) document shall be tailored in accordance with the Authorizing Official (AO)/Designated Approving Authority (DAA) from a reference CP/CPS document available from the CSfC website, for this CA product and for the specific network environment. Then it is the AO/DAA's responsibility to approve the use of this CA.

The CA for the Inner VPN components shall be located on the Red network, which allows for use of existing Enterprise CAs already operational on the Red network, following the requirements in Section 10.10.2 of this Capability Package. For networks in which an existing Enterprise CA is not available, the use of a Locally-run CA on the Red network, following the requirements in Section 10.10.3, is an acceptable alternative. If the Inner tunnel CA is an Enterprise CA already running on the Red network, no additional approval is necessary for use of this CA. For example, a solution may use an Enterprise CA (such as a CNSS-approved CA, which follows CNSSI 1300 under the NSS PKI Root CA), to issue certificates to the Inner VPN Gateway. If, however, the Inner tunnel CA uses a Locally-run CA on the Red network, the approval process given in the preceding paragraph for the Outer tunnel CA applies and must be followed.

Each VPN component shall have at least one CA signing certificate, which is used by the VPN component to authenticate to other VPN components in the solution and is sometimes referred to as a Trust Anchor. For the architecture with a Central Management site, there will be only one CA signing certificate in each VPN component. For the architecture with Multiple Independent sites, one CA signing certificate shall be installed in each Inner VPN component for each Inner Tunnel CA used in the system. Similarly, one CA signing certificate will be installed in each Outer VPN component for each Outer Tunnel CA used in the system.

Each VPN component will contain a private key that corresponds to a certificate issued by its CA, and one or more CA signing certificates as described above. Each VPN Gateway will also contain revocation information. The private key may be locally generated and shall be adequately protected. Both Inner and Outer tunnel PKIs should use ECDSA signatures within X.509 certificates, but may use RSA2048 prior to 1 October 2015. The algorithms and elliptic curves that are approved for use in this VPN solution are found in Table 4 (see Section 10.1).

The VPN Solution described here requires certificates to establish the secure tunnels between VPN components. Without certificates, the network cannot function. Thus, an out-of-band method shall be used to issue the initial certificates to the VPN components. Future rekeying, however, should take place over the network through this solution prior to the current key's expiration. The key validity period for certificates issued by Locally-run CAs shall not exceed 14 months, while the key validity period for certificates issued by an Enterprise CA shall be inherited from the Enterprise CA certificate policy. Certificate revocation information shall be updated at the same time that the VPN Gateway is rekeyed, and as directed by the AO/DAA in the case of potential compromise.

7. OVERALL SYSTEM SECURITY

This section details how the required components work together to provide overall security in the solution. Figure 3, Figure 4, and Figure 5 show the security boundary of the VPN solution for each architecture covered by this Capability Package.

An assessment of security was conducted on each of the three architectures of the solutions described in this Capability Package while making no assumptions regarding use of specific products for any of the defined components. There are several different threats to consider when evaluating the risk of transporting data over secure or unsecure networks. By examining these threats, the organization can have a better understanding of the risks they are accepting by implementing the solution and how these risks affect the Confidentiality, Integrity, and Availability of the network, systems, and data.

7.1 PASSIVE THREATS

This threat refers to internal or external actors attempting to gain information from the network without changing the state of the system. Threat actions include collecting or monitoring traffic (e.g., traffic analysis or sniffing the network) that is passing through a network in order to gain useful information through data analysis.

The security against a passive attack targeting the data in transit between the two sites is provided by the layered IPsec tunnels. To mitigate passive attacks, two layers of Suite B encryption, AES, is employed to provide confidentiality for the solution. Use of AES is approved to protect classified information, meeting IAD and CNSSP-15 guidance for adequate confidentiality. The two VPN components that are used to set up the tunnels must be independent in a number of ways (see Section 9). Due to this independence, the adversary should not be able to exploit a single cryptographic implementation to traverse both tunnels.

In the Remote Access architecture, the use of EUDs to access classified information outside of a secure facility opens the possibility that an attacker with physical access to the EUD's immediate environment could use surveillance techniques to obtain classified information without the user's

knowledge while the EUD is in use. The organization-defined terms of use tell users of EUDs what measures they must follow when using or storing the EUD to mitigate this threat.

7.2 EXTERNAL (ACTIVE) THREATS

This threat refers to outsiders gaining unauthorized access to a system or network, exfiltration of sensitive Red network data, or degradation of availability of the system or network. Threat actions include introducing viruses, malware, or worms with intentions to compromise the network or exfiltrate data or to analyze the architecture of the network or system for future attacks. Adversaries could gain access to a VPN device or EUD, and then exploit or compromise other devices on the network. Denial of Service (DoS) or Distributed DoS (DDoS) attacks compromise availability of the system, ceasing secure communication between sites. Further external threat actions would include social engineering attacks to assist attackers with gaining additional access to a network for the purpose of compromising a system or network, traffic injection or modification attacks, or replay attacks.

7.2.1 ROGUE TRAFFIC

One method for detecting rogue traffic from an external attack as it tries to pass through one or both VPN components is by having the port filtering native to each VPN Gateway enabled and configured to audit and log any traffic that is not of the format described in the configuration (see Section **Error! Reference source not found.**). It is required that the port filtering will be set up to block any traffic not coming from or going to an IP address on the network at the other site, traffic not contained in IP packets other than control plane protocols needed for network operation and approved by AO/DAA policy, and traffic going to unexpected ports. This will allow the Auditor(s) and/or the Security Administrator(s) (see Section 12) to detect whether the Outer VPN Gateway has been breached, thus providing an early warning of a potential intrusion. It will also provide detection of misconfigured Outer VPN Gateways.

Another method for detecting a potential intrusion into the solution is requiring automated configuration change detection on the Red and Gray management networks to ensure that the VPN Gateway configurations are not changed without the knowledge of the Security Administrator. The Auditor also ensures through the audit logs that all configuration changes are valid. This will counter attacks that take advantage of VPN Gateway misconfigurations.

In the Remote Access Architecture, the EUD is protected from rogue traffic through the use of traffic filtering rules configured on its interfaces connected to the Black network to drop any traffic not necessary for connecting to the infrastructure site. Appendix E provides additional guidance for how packet filtering may be implemented on the EUD.

7.2.2 MALWARE AND UNTRUSTED UPDATES

The administration devices and CAs for the Red network shall be distinct from the administration devices and CAs for the Gray network. This separation will minimize the potential of malware on a single device impacting both the Inner and Outer tunnels.

Each individual component of this solution has the capability to perform trusted updates through verification of a signature or hash to ensure that the update is from a reliable source, such as signed by the vendor. This mitigates threats of malicious users trying to push updates or code patches that affect the security of the component (and therefore system). The source of all updates and patches should be verified before installation occurs.

7.2.3 DENIAL OF SERVICE

DoS attack risks cannot be completely mitigated. The solution requires dropping all packets that are not IKE, ESP, or approved control plane protocol traffic on the appropriate interfaces, which significantly reduces the potential of flooding attacks. For customers that require more protection against these attacks, one option is the use of an optional perimeter router. This moves the responsibility to protect against a DoS attack away from this solution and back to a router that is already an established part of the customer's network. Another option for customers requiring more protection is to add additional filtering based on specifics like known network IP addresses to filter traffic from devices not included in this solution, although the feasibility of doing so in the Remote Access Architecture is limited unless the entire set of IP addresses the EUDs could be assigned is known. Other mitigations are acceptable and up to the AO/DAA to approve their use.

7.2.4 SOCIAL ENGINEERING

It is the responsibility of the customer to define the appropriate policies and training necessary to protect against Social Engineering attacks. In addition, these types of attacks generally take advantage of other attacks detailed in this section and already discussed.

7.3 INSIDER THREATS

This threat refers to an authorized or cleared person or group of people with access—physical or logical—to the network or system may act maliciously or negligently resulting in risk exposure for the organization. This threat could include poorly trained employees, curious employees, disgruntled employees, escorted personnel who gain access to the equipment, dishonest employees, or those that have the means and desire to gain escalated privileges on the network.

Threat actions include insertion or omission of data entries that result in loss of data integrity, unintentional access to an unauthorized system or network, willingly changing the configuration of the EUD, unwillingly or unknowingly executing a virus or malware, intentionally exposing

the network and systems to viruses or malware, cross contaminating a system or network with data from a higher classification to a lower classification (e.g., Secret data to Unclassified network or system), or malicious or unintentional exfiltration of classified data. Typically, the threat from insiders has the potential to cause the greatest harm to an organization, and insider attacks are also the hardest to monitor and track.

To mitigate insider threats, separation of roles within the solution is required (see Section 12). In addition, logging and auditing of security critical functionality (see Section 10.9) is required. In addition, strong authentication of the Security Administrator and Auditor are required for access to ensure accountability of these individuals. Finally, outbound filters on the VPN Gateways and EUDs are configured to look for traffic leaving the internal network that does not go through the IPsec tunnels. In scenarios that need additional assurance, an optional IDS could be deployed on the Gray network to help identify whether there is a failure, misconfiguration, or attack on the Inner or Outer VPN Gateways.

The use of a Remote Access Architecture can make detection of malicious users more difficult, since the only available means of monitoring Remote Access user behavior is to monitor their network activity. In order to mitigate this threat, an organization can implement monitoring of the Remote Access users. Additionally, organizations concerned about users misbehaving when connected remotely may wish to restrict the use of EUDs to those deemed sufficiently trustworthy.

7.4 SUPPLY CHAIN THREATS

This threat refers to an adversary gaining access to a vendor or retailer and then attempting to insert or install a modification or a counterfeit piece of hardware into a component that is destined for a U.S. Government customer in an effort to gain information or cause operational issues. This threat also includes the installation of malicious software on components of the solution. This threat is difficult to identify and test, and is increasingly more difficult to prevent or protect against since vendors build products containing components manufactured by subcontractors. It is often difficult to determine the source where different pieces of components are built and installed within the supply chain.

Threat actions include manufacturing faulty or counterfeit parts of components that can be used to disrupt system or network performance, leaving open back doors in hardware that allow attackers easy ways to attack and evade monitoring, as well as easy ways to steal data or tamper with the integrity of existing/new data. Supply Chain attacks may occur during development and production, updates, distribution, shipping, or at a warehouse or in storage.

There are doctrinal requirements placed on Implementers and System Integrators of these solutions to minimize the threat of supply chain attacks (see Sections 11 and 12).

7.5 INTEGRATOR THREATS

This threat refers to an integrator who has unrestricted access to all components within the solution prior to the customer purchasing and implementing the solution within their system. This is different than a Supply Chain threat in that these integrators have access to all components to be used in the solution, rather than only those being procured from a particular vendor.

Threat actions could include installing or configuring components in a manner that places the organization at risk for attack or open to an unknown vulnerability that may not be detected through normal tests, scans, and security counter-measures.

In order to mitigate this threat, integrators are required to be cleared to the highest level of data protected by the VPN solution. To further reduce the integrator threat, a customer may wish to use multiple integrators, such that no one integrator has access to all components of the solution.

7.6 ADDITIONAL MITIGATION INFORMATION

Traffic to the Inner VPN Gateway, including administration of the Inner VPN Gateway at Site B, is protected by two IPsec tunnels across the Black network (see Figure 3). In the Central Management Architecture, similar traffic from the Gray management network administration devices would be protected by a single IPsec tunnel across the Black network. As such, another approved encryption method from the IPsec VPN Client Protection Profile (SSHv2, IPsec, or TLS) shall be used for all traffic from the Gray management network administration device to a port on the Outer VPN Gateway at Site B. The keys to authenticate the administration device shall be at a minimum self-generated RSA/DSA key pairs, using NIST recommendations for digital signature use beyond 2013 [SP 800-131A], but also could be ECDSA key pairs using elliptic curves given in Table 4.

To avoid potential implementation weaknesses, security critical patches, such as Information Assurance Vulnerability Alerts (IAVAs), need to be applied to all components in the solution, in accordance with local policy and recommendations, thus minimizing the risks from newly discovered component vulnerabilities present in the solution. Product selection rules dictate methods for maximizing the independence between layers of the solution, which is done in part so that new vulnerabilities usually affect only one of the two layers. Only components included in applicable NSA-approved CSfC Component Lists shall be used in implementing the VPN solution (see Section 9).

The VPN Gateways will automatically perform health checks on security critical components (such as the cryptographic algorithms) during power-on self tests. By ensuring that these algorithms are not modified, the expected strength of the Suite B cryptography should be present in the solution while in use. The layering of solutions reduces the risk of single component failure breaking the security of the entire solution. However, a single component failure is likely

to result in a DoS condition. One assumption underlying this solution is that loss of availability is considered a low risk because in a DoS condition, no data has been compromised, and the problem should be noticed immediately. If availability is critical for the customer, network engineering can support further DoS protection.

8. VPN SOLUTION ARCHITECTURE AND CONFIGURATION REQUIREMENTS

In the following five sections (Sections 9 through 13), requirements applicable to the three architectures depicted in this Capability Package are documented in tables. Several requirements are only applicable to some of the architectures, and are not levied on the others. For each requirement, the tables identify which architectures the requirement is applicable to using one or more one-letter abbreviations: the Multiple Independent Sites architecture (M) (see Section 4.2.1), the Central Management Site architecture (C) (see Section 4.2.2), and the Remote Access architecture (R) (see Section 4.2.3). If a solution implements multiple architectures together, it must meet **all** of the requirements applicable to any of the architectures it implements.

Requirement priorities are specified based on guidance contained in Section 2.1.1 of the Defense Acquisition Handbook. Based on this guidance, the “Threshold or Objective” column in each table means the following:

- An objective (O) requirement specifies a feature or function that the Government desires or expects.
- A threshold (T) requirement specifies a minimum acceptable feature or function that, in the Government’s judgment, still provides the needed capabilities if the corresponding objective requirement cannot reasonably be met (e.g., due to system maturity).

In many cases, the threshold requirements also serves as the objective requirements (T=O). Where both a Threshold requirement and a related Objective requirement exist, the Objective requirement complements the Threshold requirement rather than replaces it.

9. GUIDELINES FOR SELECTING COMPONENT PRODUCTS

In this section, a series of requirements are given for maximizing the independence between the components within the solution. This will increase the level of effort required to compromise this solution.

Table 1. Product Selection Requirements

Req #	Requirement Description	Architectures	Threshold / Objective
PS1	Vendor Diversity – The Inner and Outer VPN Gateways shall come from different vendors. One vendor cannot be a subsidiary of the other.	M, C, R	T=O
PS2	Hardware Platform Diversity – The Inner and Outer VPN Gateways shall be run on separate physical hardware platforms.	M, C, R	T=O
PS3	Operating System (OS) Diversity – The Inner and Outer VPN Gateways shall not use the same OS for critical IA security functionality. Differences between Service Packs (SP) or version numbers for a particular vendor's OS do not provide adequate diversity.	M, C, R	T=O
PS4	The Outer tunnel CA should come from a different vendor than the CA used by the Inner tunnel.	M, C, R	O
PS5	The Inner and Outer VPN Clients shall come from different vendors. One vendor cannot be a subsidiary of the other.	R	T=O

It would also be beneficial to ensure that the IPsec cryptographic libraries being used to establish the VPN tunnel are unique. In some cases, it may not be possible to know which library is used in the VPN components, but if that information is available, then the two VPN components should use different cryptographic libraries.

The products that are approved for use in this solution are listed on the IAD/CSfC website. No single product shall be used to protect classified information alone. The only approved methods for using COTS products to protect classified information follow the requirements outlined in a Capability Package. Products shall be selected for the VPN solution from the Component Lists given in the following table.

Table 2. CSfC Component Lists for the VPN Products

Product	Component List
Inner VPN Gateway	IPsec VPN Gateway
Outer VPN Gateway	IPsec VPN Gateway
Inner VPN Client	IPsec VPN Client
Outer VPN Client	IPsec VPN Client
Outer Tunnel Certificate Authority	Certificate Authority
Inner Tunnel Certificate Authority	Certificate Authority (or Enterprise CA)

It is preferred that the Inner Tunnel CA be part of a customer's enterprise keying solution. In that case, the CA will not be selected from a Component List because it already exists on the Red network. If there is no existing Enterprise CA, however, the Inner Tunnel CA should also be selected from the Certificate Authority Component List.

10. CONFIGURATION

Once the products for the solution are selected, the next step is setting up the components and configuring them in a secure manner. This section consists of generic guidance for how to configure the components of the VPN solution.

10.1 OVERALL SOLUTION REQUIREMENTS

Table 3. Overall Solution Requirements

Req #	Requirement Description	Architectures	Threshold / Objective
SR1	The Gray management network traffic shall be separate from the data traffic on the Gray network; use of dedicated physical management ports on the VPN Gateways provides the necessary separation. (See Section 4.2)	M, C, R	T=O
SR2	Fundamental network architecture components, such as DNS and NTP that are not explicitly included in the solution, should be located on the inside network (Gray network for Outer VPN Components and Red network for Inner VPN Components). (See Section 4.2)	M, C, R	O
SR3	Sites that need to communicate shall ensure that the VPN Gateways selected by each site are interoperable. (See Section 4.2.1)	M, C	T=O
SR4	The time of day on each component in the solution shall be synched with the Administration device and CA on the corresponding (Red or Gray) network. This is necessary to ensure that certificates are accepted and to ensure adherence to the validity period of the certificate. Security Administrators shall employ adequate defenses of their time servers.	M, C, R	T=O
SR5	The VPN clients selected for End User Devices shall be interoperable with the corresponding VPN Gateways.	R	T=O

10.2 CONFIGURATION REQUIREMENTS FOR ALL VPN COMPONENTS

Table 4. Approved Suite B Algorithms

Security Service	Algorithm Suite 1	Algorithm Suite 2	Specifications
Overall Level of Security	128 bits	192 bits	
Confidentiality (Encryption)	AES-128	AES-256	FIPS PUB 197
Authentication (Digital Signature)	ECDSA over the curve P-256 with SHA-256	ECDSA over the curve P-384 with SHA-384	FIPS PUB 186-3
	RSA 2048 (prior to 1 October 2015)	N/A	FIPS PUB 186-3
Key Exchange/ Establishment	ECDH over the curve P-256 (DH Group 19)	ECDH over the curve P-384 (DH Group 20)	NIST SP 800-56A IETF RFC 6379 Suite B Cryptographic Suites for IPsec (IKEv2)
Integrity (Hashing)	SHA-256	SHA-384	FIPS PUB 180-4
Can protect	Up to Secret	Up to Top Secret	

Table 5. Configuration Requirements for Both VPN Components

Req #	Requirement Description	Architectures	Threshold / Objective
CR1	The proposals offered in the course of establishing the IKE Security Association (SA) and the ESP SA for the Inner and Outer Tunnels shall be configured to offer algorithm suite(s) containing only Suite B algorithms (see Table 4 or www.nsa.gov). As such, algorithm suites containing non-Suite B algorithms or parameters shall be removed from the list of algorithms offered during negotiation.	M, C, R	T=O
CR2	The VPN components shall be configured to restrict the IP address range for the network administration device to the smallest range possible.	M, C, R	T=O
CR3	Default accounts, passwords, community strings, and other default access control mechanisms for the administration of the VPN components shall be changed or eliminated.	M, C, R	T=O
CR4	The default, self-signed or proprietary device certificates, which are frequently preinstalled by the vendor, for any VPN components shall not be used for establishing SAs and removed if possible.	M, C, R	T=O
CR5	A unique device certificate shall be loaded onto each VPN component along with the corresponding CA (signing)	M, C, R	T=O

Req #	Requirement Description	Architectures	Threshold / Objective
	certificate. The device certificate shall be used for component authentication during IKE; authentication shall include a check against certificate revocation information. The private key shall be stored on the VPN Gateway and shall not be accessible through any interface.		
CR6	The VPN Gateways shall be configured so that the only approved physical paths leaving the Red network are through a VPN solution in accordance with this Capability Package or via an approved NSA-certified device (such as a HAIPE) ¹ .	M, C, R	T=O
CR7	Each VPN Gateway shall be configured to audit and log when unauthorized access attempts and/or privilege escalation occur or are identified (see Section 10.9).	M, C, R	T=O
CR8	At least one of the two VPN Gateways shall be configured to use the IKEv2 key exchange. In the Remote Access Architecture, the corresponding VPN clients shall be configured likewise.	M, C, R	T=O
CR9	For solutions using IPv4, the external interface of each VPN component shall drop all packets that use IP options (e.g., if the first byte is not 0x45, then the packet shall be dropped and may be audited). A similar requirement is not placed on IPv6 instantiations.	M, C, R	T=O
CR10	The use of at least one outer interface loopback address is recommended. When present, the VPN Gateway's loopback address shall be used as the source address for management functions. This is advantageous instead of handling the numerous physical interface addresses.	M, C, R	T=O
CR11	Passwords for administrative access shall be stored cryptographically protected in the VPN component's configuration.	M, C, R	T=O
CR12	Each VPN Gateway shall be configured to audit and log when remote access connections are established.	M, C, R	T=O
CR13	Each VPN Gateway shall be configured to detect when two or more simultaneous connections are established by the same device certificate.	M, C, R	T=O

¹In some cases, the customer will need to communicate with other sites that have NSA-certified Government off-the-Shelf (GOTS) equipment. In particular, it is okay for a given site to have both an egress path via an NSA-certified device and an egress path via a layered COTS solution conforming to this Capability Package. This will allow a site to communicate with remote sites that use either solution.

10.3 ADDITIONAL REQUIREMENTS FOR INNER VPN COMPONENTS

Table 6. Additional Requirements for Inner VPN Components

Req #	Requirement Description	Architectures	Threshold / Objective
IR1	<p>The Inner VPN component shall use the following protocols and algorithms for creating all VPN tunnels. Algorithms shall be selected from within a single Algorithm Suite column in Table 4.</p> <ul style="list-style-type: none"> • IKEv1 (RFC 2409) key exchange in Main Mode on Phase 1 or IKEv2 (RFC 5996) key exchange • All Diffie-Hellman (DH) key exchanges performed as part of IKE/IPsec shall utilize DH Group 19 or DH Group 20 • Certificates based on the NIST P-256 or P-384 Elliptic Curve, or RSA2048 for up to SECRET data prior to 1 October 2015. • SHA-256 or SHA-384 for a hash function • AES-128 or AES-256 in Cipher Block Chaining for IKE encryption • Tunnel mode IPsec or Transport mode IPsec with an associated IP tunneling protocol (e.g., GRE) using AES-128 or AES-256 with Galois Counter Mode or Cipher Block Chaining (CBC) for ESP encryption. In future versions of the Capability Package, CBC mode will no longer be an option for ESP encryption. This change will be made no later than 2016. • IKE SA lifetime set to 24 hours • ESP SA lifetime set to 8 hours 	M, C, R	T=O
IR2	<p>The packet size for packets leaving the external interface of the Inner VPN component shall be configured to keep the packets from being fragmented and impacting performance. This requires proper configuration of the MTU (for IPv4) or PMTU (for IPv6) and should consider the Black network and Outer VPN component MTU/PMTU values to achieve this.</p>	M, C, R	T=O

10.4 ADDITIONAL REQUIREMENTS FOR OUTER VPN COMPONENTS

Table 7. Additional Requirements for Outer VPN Components

Req #	Requirement Description	Architectures	Threshold / Objective
OR1	<p>The Outer VPN component shall use the following protocols and algorithms for creating all VPN tunnels. Algorithms shall be selected from within a single Algorithm Suite column in Table 4.</p> <ul style="list-style-type: none"> • IKEv1 (RFC 2409) key exchange in Main Mode on Phase 1 or IKEv2 (RFC 5996) key exchange 	M, C, R	T=O

Req #	Requirement Description	Architectures	Threshold / Objective
	<ul style="list-style-type: none"> All Diffie-Hellman (DH) key exchanges performed as part of IKE/IPsec shall utilize DH Group 19 or DH Group 20. Certificates based on the NIST P-256 or P-384 Elliptic Curve, or RSA2048 for up to SECRET data prior to 1 October 2015. SHA-256 or SHA-384 for a hash function AES-128 or AES-256 in Cipher Block Chaining for IKE encryption Tunnel mode IPsec using AES-128 or AES-256 with Galois Counter Mode or Cipher Block Chaining for ESP encryption. In future versions of the Capability Package, CBC mode will no longer be an option for ESP encryption. This change will be made no later than 2016. IKE SA lifetime set to 24 hours ESP SA lifetime set to 8 hours 		
OR2	All traffic originating in the Red or Gray networks going out the external interface on the Outer VPN Gateway shall be encrypted in accordance with this Capability Package.	M, C, R	T=O
OR3	All traffic originating from the EUD, with the exception of traffic necessary for the EUD to connect to the Black network (e.g. DHCP) and locate the Outer VPN Gateway (e.g. DNS lookup of the Outer VPN Gateway's IP address), shall be encrypted in accordance with this Capability Package.	R	T=O
OR4	If one or more virtual machines are used on the EUD to separate the Inner and Outer VPN Clients, then the Outer VPN Client shall not run on the host operating system.	R	T=O

10.5 REQUIREMENTS FOR END USER DEVICES

Table 8. Requirements for End User Devices

Req #	Requirement Description	Architectures	Threshold / Objective
EU1	The EUD shall implement a Thin Client that is configured to prohibit storage of user data from the Red network on the device.	R	T=O
EU2	The EUD shall prohibit the use of external data storage media (e.g. USB storage devices, DVDs).	R	T=O
EU3	The Inner and Outer VPN Clients on the EUD shall use separate private key stores.	R	T=O
EU4	The Inner and Outer VPN Clients on the EUD shall be implemented on separate IP stacks.	R	T=O

Req #	Requirement Description	Architectures	Threshold / Objective
EU5	Unless the EUD is remotely administered as specified in requirement RA3, it shall be updated only through re-provisioning.	R	T=O
EU6	The VPN clients shall be initially keyed within a physical environment certified to protect the highest classification level of the VPN solution network. If the EUD is remotely administered as specified in requirement RA3, rekeying shall be done over the VPN solution network prior to expiration of keys. If rekeying is not completed prior to expiration of keys, or if remote administration of the EUD is not performed, they will need to be rekeyed through the same process as initial keying.	R	T=O
EU7	Remote users shall be required to successfully perform two-factor authentication prior to gaining access to services on the Red network. The services shall not transmit any classified data to the EUD until user authentication succeeds.	R	T=O
EU8	The EUD shall implement FIPS-140-2 (or later) compliant Full Disk Encryption.	R	T=O
EU9	The EUD should implement the BIOS security guidelines specified in NIST SP 800-147.	R	O
EU10	Upon discovering an EUD is lost or stolen a remote access user shall immediately report the incident to their System Administrator and Certificate Authority Administrator.	R	T=O
EU11	Upon notification of a lost or stolen EUD, the Certificate Authority Administrators shall immediately update the Certificate Revocation List (CRL) in the Inner and Outer VPN Gateway.	R	T=O
EU12	EUDs shall be provisioned in the secure facility where the Certificate Authorities are physically located. The provisioning process includes assigning identifiers to the EUDs, installing required applications, configuring the device's policy and settings, and loading certificates and keying material.	R	T=O
EU13	<p>All Remote Access users shall sign an organization-defined user agreement before being authorized to use an EUD. At a minimum, the user agreement shall include each of the following:</p> <ul style="list-style-type: none"> • Consent to monitoring • OPSEC guidance • Required physical protections to employ when operating and storing the EUD • Restrictions for when and where the EUD may be used • Verification of IA Training • Verification of appropriate clearance • Justification for Access 	R	T=O

Req #	Requirement Description	Architectures	Threshold / Objective
	<ul style="list-style-type: none"> Requester information and organization Account Expiration Date User Responsibilities 		
EU14	EUDs shall be provisioned over wired connections.	R	T=O
EU15	The Certificate Authority Administrators shall immediately update the Certificate Revocation List (CRL) when two or more simultaneous connections are established by the same device certificate.	R	T=O
EU16	Software, settings, keys, and all other configuration data persistently stored on the EUD shall be unclassified.	R	T=O

10.6 PORT FILTERING REQUIREMENTS FOR VPN COMPONENTS

Table 9. Port Filtering Requirements for VPN Components

Req #	Requirement Description	Architectures	Threshold / Objective
PF1	For all interfaces connected to the Gray or Black networks, traffic filtering rules shall be applied to both inbound and outbound traffic, such that only IKE, ESP, and control plane protocols approved by policy are allowed. All other data shall be blocked and may be audited. In addition, traffic filtering rules may be applied based on known VPN Gateway addresses to further protect against unknown IPsec traffic.	M, C, R	T=O
PF2	Any service or feature that allows the Outer VPN component or the EUD to contact a third party server (such as one maintained by the manufacturer) shall be disabled or blocked.	M, C, R	T=O
PF3	Outer VPN Gateways shall block all data (by ports and IP addresses) on their Gray Management network interface that is not necessary for the management of Outer VPN Gateways.	M, C, R	T=O
PF4	The Gray management network traffic shall be separate from the data traffic on the Gray network; use of dedicated management ports on the VPN Gateways provides the necessary separation.	M, C, R	T=O
PF5	Multicast messages received on external interfaces of the Outer VPN component shall be dropped and may be logged.	M, C, R	T=O
PF6	For all Inner VPN Gateway interfaces connected to the Red network, traffic filtering rules shall be applied to both inbound and outbound traffic, such that only Thin Client and remote management protocols are allowed to be sent to and received from an EUD. All other data to or from an EUD shall be blocked and may be audited.	R	T=O

10.7 CONFIGURATION CHANGE DETECTION REQUIREMENTS

Table 10. Configuration Change Detection Requirements

Req #	Requirement Description	Architectures	Threshold / Objective
CM1	A baseline configuration for all Inner and Outer VPN components shall be maintained by the System Administrator and the Auditor.	M, C, R	T=O
CM2	An automated process shall ensure that configuration changes are logged. This log entry shall include the specific changes to the configurations.	M, C, R	T=O

10.8 REQUIREMENTS FOR VPN COMPONENT ADMINISTRATION

Only authorized Security Administrators will be allowed to administer the VPN components. RA1 and RA3 ensure that administrator authentication to the component occurs prior to any administrative function taking place. The VPN solution will be used as transport for the SSHv2, IPsec, or TLS data from the administrative machine to the VPN component. This means that to remotely administer an Outer VPN component, the existing tunnel between Outer VPN components will carry the SSH, IPsec, or TLS data and in order to remotely administer an Inner VPN component, the SSH, IPsec, or TLS data will travel inside the two tunnels to reach the remote Inner VPN component.

Table 11. Requirements for VPN Component Administration

Req #	Requirement Description	Architectures	Threshold / Objective
RA1	<p>Inner and Outer VPN Gateway administration management shall be performed from a VPN administration device (either on the Gray management network for the Outer VPN Gateway or on the Red network for the Inner VPN Gateway) as follows:</p> <p>Remotely using the SSHv2 protocol as specified in RFCs 4252-4254, the IPsec protocol as specified in RFCs 2409, 4302, 4303, 4307, 4308, 5996, and 6379, or the TLS protocol as specified in RFCs 5246 and 6460. The SSH, IPsec, or TLS data, as with all data, shall also be protected by the IPsec VPNs. In the case of the Outer VPN Gateway, the SSH, IPsec, or TLS data will only be protected by one IPsec VPN tunnel that is also part of the double tunnel between the Red networks. Additional information about key sizes and options for using these protocols is available at [NSA Suite B].</p>	M, C, R	T=O
RA2	The Admin workstations shall be dedicated for the purposes given in Section 5.4 and properly configured according to local policy and U.S. Government guidance (e.g., Defense Information Systems Agency (DISA) gold disk, NSA	M, C, R	T=O

Req #	Requirement Description	Architectures	Threshold / Objective
	guidelines). Adequate procedures shall exist for handling, storage, and lifecycle support. Antivirus software shall be running on all Admin workstations.		
RA3	If End User Devices are remotely administered, then Inner and Outer VPN Client administration management shall be performed from a VPN administration device (either on the Gray management network for the Outer VPN Client or on the Red network for the Inner VPN Client) as follows: Remotely using the SSHv2 protocol as specified in RFCs 4252-4254, the IPsec protocol as specified in RFCs 2409, 4302, 4303, 4307, 4308, 5996, and 6379, or the TLS protocol as specified in RFCs 5246 and 6460. The SSH, IPsec, or TLS data, as with all data, shall also be protected by the IPsec VPNs. In the case of the Outer VPN Client, the SSH, IPsec, or TLS data will only be protected by one IPsec VPN tunnel that is also part of the double tunnel between the Red networks. Additional information about key sizes and options for using these protocols is available at [NSA Suite B].	R	T=O

10.9 AUDITING REQUIREMENTS

Table 12. Auditing Requirements

Req #	Requirement Description	Architectures	Threshold / Objective
AU1	<p>At a minimum, the following set of auditable events shall be logged by the VPN Gateways on a continuous basis and these logs shall be monitored by the Security Administrator and Auditor on a weekly basis:</p> <ul style="list-style-type: none"> • All modifications to the audit configuration and all actions performed on the audit log (off-loading, deletion, etc.). • All actions involving identification and authentication. • Attempts to perform an unauthorized action (read, write, execute, delete, etc.) on an object. • All actions performed by a user with super privileges (auditor, administrator, etc.) and any escalation of user privileges. • Any changes to the baseline configuration of a product. • Certificate operations including generation, loading, or revoking of certificates. • Changes to time. • Receipt of unexpected data on any interface directly connected to the Gray data or management networks. • All built-in self-test results, which may indicate 	M, C, R	T=O

Req #	Requirement Description	Architectures	Threshold / Objective
	failures in cryptographic functionality.		
AU2	The set of auditable events specified in the CPS shall be monitored and logged within the outer-tunnel CAs used for VPN Gateways on a continuous basis when in use.	M, C, R	T=O
AU3	<p>The following information shall be recorded for each audit event:</p> <ul style="list-style-type: none"> • Date and time of the event • Identifier for the event • Type of event • Success or failure of event to include failure code, when available • Subject identity • Source address for network based events • User and role identification for role based events 	M, C, R	T=O

10.10 KEY MANAGEMENT REQUIREMENTS

10.10.1 PKI REQUIREMENTS FOR VPN COMPONENTS

Table 13. PKI Requirements for VPN Components

Req #	Requirement Description	Architectures	Threshold / Objective
KM1	The key sizes and algorithms used for the Inner and Outer VPN Components shall be as specified in Table 4 of this VPN Capability Package.	M, C, R	T=O
KM2	The CAs shall be located on separate networks (specifically, the Red and Gray management networks). A separate CA shall support the Inner and Outer VPN, such that certificates are not generated by a single common CA.	M, C, R	T=O
KM3	Both the Inner and Outer tunnel CAs shall operate under a CPS that is formatted in accordance with Internet Engineering Task Force (IETF) Request for Comments (RFC) 3647.	M, C, R	T=O
KM4	Both Inner and Outer tunnel CAs shall use ECDSA signatures within X.509 certificates.	M, C, R	T=O
KM5	Inner tunnel VPN Components shall only trust an Inner tunnel CA used within the solution.	M, C, R	T=O
KM6	Outer tunnel VPN Components shall only trust an Outer tunnel CA used within the solution.	M, C, R	T=O

Req #	Requirement Description	Architectures	Threshold / Objective
KM7	All public/private key pairs and certificates for VPN Components shall be used for authentication (i.e., signature) only. VPN Component keys shall not be escrowed.	M, C, R	T=O
KM8	The VPN Gateways shall be initially keyed within a physical environment certified to protect the highest classification level of the VPN solution network. Rekeying shall be done over the VPN solution network prior to expiration of keys. The certification revocation information shall be updated at the same time as the gateway is rekeyed. If rekeying is not completed prior to expiration of keys, they will need to be rekeyed through the same process as initial keying.	M, C, R	T=O

10.10.2 ENTERPRISE PKI REQUIREMENTS

Table 14. Enterprise PKI Requirements

Req #	Requirement Description	Architectures	Threshold / Objective
KM9	The Enterprise CA shall assert a registered Object Identifier (OID) to all of its VPN Components.	M, C, R	T=O
KM10	The Enterprise CA shall be located on the Red network and be approved to issue certificates to VPN Components (such as one that follows CNSSI 1300 under the NSS PKI Root CA).	M, C, R	T=O

10.10.3 LOCALLY-RUN PKI REQUIREMENTS

Table 15. Locally-Run PKI Requirements

Req #	Requirement Description	Architectures	Threshold / Objective
KM11	Locally-run CAs shall be chosen from the CSfC CA Component List of NSA-approved CA devices. The AO/DAA will need to approve the use of this CA, which will require a CP and CPS (see KM3) [CP/CPS reference document].	M, C, R	T=O
KM12	All Locally-run CAs used for VPN Components are subject to audit requirements against the CPS as defined in KM3.	M, C, R	T=O
KM13	Locally-run CAs shall only issue certificates to the appropriate VPN components or to support its own operations.	M, C, R	T=O
KM14	Certificate revocation information shall be made available by posting the data to a repository or service that is available for the VPN Components.	M, C, R	T=O
KM15	The workstation used to manage the Locally-run CA shall be dedicated for this purpose and properly configured according to local policy and U.S. Government guidance (e.g., DISA gold disk, NSA guidelines). Adequate procedures shall exist	M, C, R	T=O

Req #	Requirement Description	Architectures	Threshold / Objective
	for handling, storage, and lifecycle support.		
KM16	Locally-run CAs shall have a limited name space to issue certificates. Names shall be unique.	M, C, R	T=O
KM17	The key validity period for certificates issued by Locally-run CAs shall not exceed 14 months. New certificates may be issued as needed in accordance with local policy.	M, C, R	T=O

11. GUIDANCE FOR THE USE AND HANDLING OF SOLUTIONS

The following requirements shall be followed regarding the use and handling of the solution.

Table 16. Guidance for the Use and Handling of Solutions

Req #	Requirement Description	Architectures	Threshold / Objective
GD1	All components of the solution, with the exception of the EUD when powered off, shall be physically protected as classified devices, classified at the level of the network in the solution with the highest classification. Only authorized and appropriately cleared (or escorted) administrators and security personnel shall have physical access to the infrastructure components. Only authorized and appropriately cleared users, administrators, and security personnel shall have physical access to the EUD.	M, C, R	T=O
GD2	All components of the solution shall be disposed of as classified devices, unless declassified using AO/DAA-authorized procedures.	M, C, R	T=O
GD3	Acquisition and procurement documentation shall not include information about how the equipment will be used, to include that it will be used to protect classified information.	M, C, R	T=O
GD4	Solution owner shall allow, and fully cooperate with, NSA or its authorized agent to perform an IA compliance audit (including, but not limited to, inspection, testing, observation, interviewing) of the solution implementation to ensure it meets the current version of the Capability Package.	M, C, R	T=O
GD5	The AO/DAA will ensure that a compliance audit shall be conducted every 3 years against the latest version of the VPN Capability Package, and the results shall be provided to the AO/DAA. In addition, when a new version of the VPN Capability Package is published by NSA, the AO/DAA shall ensure compliance against this new Capability Package within 6 months.	M, C, R	T=O
GD6	Solution implementation information, which was provided to NSA during solution registration, shall be updated every 12 (or less) months (see Section 13.3).	M, C, R	T=O

Req #	Requirement Description	Architectures	Threshold / Objective
GD7	<p>Audit log data for security critical events (see Auditing requirements in Section 10.9) shall be handled according to the following requirements.</p> <ol style="list-style-type: none"> 1. Audit logs shall be reviewed by the Auditor at least weekly (or more frequently if required by the local AO/DAA) to look for unauthorized access. 2. Audit log data shall be maintained for a minimum of 1 year. 3. During the quarterly review of the audit data, the amount of storage remaining for audit events shall be assessed in order to ensure that adequate memory space is available to continue recording new audit events. 4. Audit data shall be frequently offloaded to a backup storage medium in order to facilitate compliance with requirements 2 and 3 above. 	M, C, R	T=O
GD8	A set of procedures shall be developed to provide guidance for identifying and reporting security incidents associated with the audit events to the proper authorities and to the data owners.	M, C, R	T=O
GD9	<p>A procedure shall be developed for ensuring continuity of operations for the auditing capability. This plan shall include each of the following as a minimum.</p> <ul style="list-style-type: none"> • A mechanism or method for determining when the audit log is reaching its maximum storage capacity. • A mechanism or method for off-loading audit log data for long term storage. • A mechanism or method for responding to an overflow of audit log data within a product. • A mechanism or method for ensuring that the audit log can be maintained during power events. 	M, C, R	T=O
GD10	Passwords – Strong passwords shall be used that comply with the requirements of the local security authority.	M, C, R	T=O
GD11	Patching of components – It is expected that security critical patches (such as IAVAs) shall be made to all components in the solution. Local policy shall dictate how the Security Administrator will install patches on the Red, Gray, and Black networks.	M, C, R	T=O
GD12	TEMPEST – The VPN solution does not provide any TEMPEST protections, thus any TEMPEST requirements shall comply with local TEMPEST policy.	M, C, R	T=O

Additional policy can be found in Section 12 below.

12. ROLE-BASED PERSONNEL REQUIREMENTS

The roles required to administer and maintain the solution are defined below, along with doctrinal requirements for these roles.

Security Administrator – The Security Administrator shall be responsible for maintaining, monitoring, and controlling all security functions for the entire suite of products composing the VPN solution within a single site. Security Administrator duties include but are not limited to:

- 1) Ensuring that the latest security critical software patches and updates (such as IAVAs) are applied to each product.
- 2) Documenting and reporting security-related incidents to the appropriate authorities.
- 3) Coordinating and supporting product logistic support activities including integration and maintenance. Some logistic support activities may require that the Security Administrator escort uncleared personnel.
- 4) Employing adequate defenses of auxiliary network devices to enable proper and secure functionality of the VPN solution.
- 5) Ensuring that the implemented VPN solution remains compliant with the latest version of this Capability Package.
- 6) Provisioning and maintaining EUDs in accordance with this Capability Package for implementations which include the Remote Access Architecture.

Certificate Authority Administrator (CAA) – The CAA shall be responsible for maintaining, monitoring, and controlling all security functions for the CA products. CAA duties include but are not limited to:

- 1) Administering the CA, including authentication of all components requesting certificates.
- 2) Maintaining and updating the Certificate Revocation List.
- 3) Provisioning and maintaining EUD certificates in accordance with this Capability Package for implementations which include the Remote Access architecture.

Auditor – The Auditor shall be responsible for reviewing the actions performed by the Security Administrator and CAA and events recorded in the audit logs to ensure that no action or event represents a compromise to the security of the wired VPN solution. The role of Auditor and Security Administrator shall not be performed by the same individual. Auditor duties include but are not limited to:

- 1) Reviewing, managing, controlling, and maintaining security audit log data.
- 2) Documenting and reporting security related incidents to the appropriate authorities.

- 3) The Auditor will only be authorized access to the Outer and Inner admin components.

Solution Integrator – In certain cases, an external integrator may be hired to implement a VPN solution based on this Capability Package. Solution Integrator duties may include but are not limited to:

- 1) Acquiring the products that compose the solution.
- 2) Configuring the VPN solution in accordance with this Capability Package.

Remote User – In implementations which utilize the Remote Access architecture, a remote user may operate an EUD from physical locations not owned or operated by the government. The remote user shall be responsible for operating the EUD in accordance with this Capability Package and an organization defined user agreement. Remote User duties include, but are not limited to:

- 1) Ensuring the EUD is only operated in physical spaces which comply with the end user agreement.
- 2) Alerting the Security Administrator immediately upon an EUD being lost, stolen, or suspected of being tampered with.

Additional policies related to the personnel that perform these roles in a VPN Solution are as follows:

Table 17. Role-Based Personnel Requirements

Req #	Requirement Description	Architectures	Threshold / Objective
GD13	The Security Administrator, CAAs, Auditor, Remote User, and all Solution Integrators shall be cleared to the highest level of data protected by the VPN solution.	M, C, R	T=O
GD14	When a previously established CA is used in the solution, the CAA already in place may also support this solution provided they meet GD13.	M, C, R	T=O
GD15	The Security Administrator, CAA, and Auditor roles shall be performed by different people.	M, C, R	T=O
GD16	All Security Administrators, CAAs, Remote Users, and Auditors shall meet local information assurance training requirements.	M, C, R	T=O
GD17	The CAA(s) for the Inner tunnel shall be different from the CAA(s) for the Outer tunnel.	M, C, R	T=O

13. INFORMATION TO SUPPORT AO/DAA

This section details items that likely will be necessary for the customer to obtain approval from the system AO/DAA. The customer and AO/DAA have obligations to perform the following:

- The customer, possibly with support from a System Integrator, instantiates a solution implementation that follows the NSA-approved Capability Package.
- The customer has a testing team develop a Test Plan and perform testing of the VPN solution, see Sections 13.1 and 14.
- The customer has system certification and accreditation performed using the risk assessment information referenced in Section 13.2.
- The customer provides the results from testing and system certification and accreditation to the AO/DAA for use in making an approval decision. The AO/DAA is ultimately responsible for ensuring that all requirements from the Capability Package have been properly implemented.
- The customer registers the solution with NSA and re-registers yearly to validate its continued use as detailed in Section 13.3.
- Customers who want to use a variant of the solution detailed in this Capability Package will contact NSA to determine ways to obtain NSA approval.
- The AO/DAA will ensure that a compliance audit shall be conducted every 3 years against the latest version of the VPN Capability Package, and the results shall be provided to the AO/DAA.
- The AO/DAA will ensure that certificate revocation information is updated on all the VPN gateways in the solution in the case of a compromise.
- The AO/DAA will ensure that any Layer 2 or Layer 3 control plane protocols that are used in the solution are necessary for the operation of the network and that local policy supports their use.

The system AO/DAA maintains configuration control of the approved solution implementation over the lifecycle of the solution. Additionally, the AO/DAA shall ensure that the solution remains properly configured, with all required security updates implemented.

13.1 SOLUTION TESTING

This section provides a framework for a Test and Evaluation (T&E) plan and procedures to validate the implementation of a VPN solution. This T&E will be a critical part of the approval

process for the AO/DAA, providing a robust body of evidence that shows compliance with this Capability Package.

The security features and operational capabilities associated with the use of the solution shall be tested. The following is a general high-level methodology for developing the test plan and procedures and for the execution of those procedures to validate the implementation and functionality of the VPN solution. The entire solution, to include each component described in Section **Error! Reference source not found.**, is addressed by this test plan.

- 1) Set up the baseline network architecture and configure all components.
- 2) Document the baseline network architecture configuration. Include product model and serial numbers, and software version numbers as a minimum.
- 3) Develop a Test Plan for the specific implementation using the test objectives from Section 14. Any additional requirements imposed by the local AO/DAA should also be tested, and the Test Plan shall include tests to ensure that these requirements do not interfere with the security of this solution as described in this Capability Package.
- 4) Perform testing using the test plan derived in Step 3. Network testing will consist of both Black Box testing and Gray Box testing. A two-person testing approach should be used to administer the tests. During test execution, security and non-security related discrepancies with the solution shall be documented.
- 5) Compile findings, to include comments and vulnerability details as well as possible countermeasure information, into a Final Test Report to be delivered to the AO/DAA for approval of the solution.

The following testing requirements have been developed to ensure that the VPN solution functions properly and meets the configuration requirements from Section **Error! Reference source not found.** Testing of these requirements should be used as a minimum framework for the development of the detailed test plan and procedures.

Table 18. Test Requirements

Req #	Requirement Description	Architectures	Threshold / Objective
TR1	Ensure end-to-end communication.	M, C, R	T=O
TR2	Verify ability to manage all VPN Gateways in the solution.	M, C, R	T=O
TR3	Document the physical layout of the VPN solution implementation.	M, C, R	T=O

13.2 RISK ASSESSMENT

The risk assessment of the VPN solution presented in this Capability Package focuses on the types of attacks that are feasible against this solution and the mitigations that can be employed. Customers should contact their NSA/IAD Client Advocate to request this document, or visit the SIPRNet CSfC site for information. The process for obtaining the risk assessment is available on the SIPRNet CSfC website. The AO/DAA shall be provided a copy of the NSA risk assessment for their consideration in approving the use of the solution.

13.3 REGISTRATION OF SOLUTIONS

All customers using CSfC solutions to protect information on National Security Systems shall register their solution with NSA prior to operational use. This registration will allow NSA to track where VPN Capability Package solutions are instantiated and to provide AO/DAAs at those sites with appropriate information, including any significant vulnerabilities that may be discovered in components/architectures approved for these solutions. The CSfC solution registration process is available at http://www.nsa.gov/ia/programs/csfc_program.

Solutions designed to this Capability Package may be used for one year, and must then be revalidated against the current Capability Package. Approved Capability Packages will be reviewed twice a year, or as events warrant. Notification of these updates will be provided to all registered users of the Capability Package.

14. TESTING REQUIREMENTS

This section contains the specific tests that allow the Security Administrator or System Integrator to ensure that they have properly configured the solution. These tests may also be used to provide evidence to the AO/DAA regarding compliance of the solution with this Capability Package. Note that the details of the procedures are left up to the final developer of the test plan in accordance with AO/DAA-approved network procedures. The AO/DAA is ultimately responsible for ensuring that all requirements from the Capability Package have been properly implemented.

14.1 PRODUCT SELECTION

This section contains a procedure to verify that the Inner and Outer VPN Gateways were selected to ensure independence in several important features.

Requirements being tested: PS1through PS5, SR3, SR5

Procedure Description:

- 1) For each VPN Gateway, perform the following:

- a) Inspect that the Inner and Outer VPN Gateways came from different manufacturers. (PS1)
 - b) Inspect that the Inner and Outer VPN Gateways are running on separate hardware platforms. (PS2)
 - c) Inspect that the Inner and Outer VPN Gateways are running differing Operating Systems. (PS3)
 - d) Inspect that the Inner and Outer tunnel CAs came from different manufacturers. (PS4)
- 2) Inspect that the Inner and Outer VPN clients came from different manufacturers. (PS5) For sites requiring interoperability, ensure that VPN products selected for each tunnel can be configured to communicate using the requirements specified in this Capability Package. (SR3)

Expected Result:

The results of the inspection should reveal that the VPN components conform to the VPN CP; results are pass/fail.

14.2 PHYSICAL LAYOUT OF SOLUTION

This section contains a procedure to create an accurate record of the physical components composing the VPN solution (including workstations, VPN Gateways, CA, and wiring). The test will also ensure that the physical implementation of the VPN solution matches one of the architectures given in the VPN Capability Package.

Requirements being tested: SR1, SR2, CR6, TR3

Procedure Description:

- 1) Record all physical connections between the components in the VPN solution, including interfaces used on the VPN Gateways, connections used on workstations, and wiring. (SR1, SR2, TR3)
- 2) Compare this record with the architectures given in the VPN Capability Package and ensure what is implemented matches one of the architectures. (TR3)
- 3) Ensure that there are no wireless connections connected to the solution that are not included in this Capability Package, which may allow for traffic to leave the Red or Gray network in a manner that does not go through the VPN solution (or an NSA-certified encryptor). (CR6)

- 4) Ensure that the Gray management network is connected through a dedicated management port on the Outer VPN Gateway that is separate from the port used for the Gray data network. (SR1)
- 5) Verify that the physical location of any network architecture component for the Outer VPN Gateway is located on the Gray management network. Similarly, these components for the Inner VPN Gateway will be located on the Red network. (SR2)

Expected Result:

For Step 2, the record compiled in Step 1 should match either the Central Management, Multiple Independent Site, or Remote Access Architectures given in this Capability Package. For Step 3, there should be no extraneous wireless connections allowing data to leave the Red or Gray networks besides through the VPN solution (or an NSA-certified encryptor).

14.3 END USER DEVICE CONFIGURATIONS

This section contains a procedure to ensure that the configurations for all the EUDs in the VPN solution follow the requirements given in this Capability Package.

Requirements being tested: EU1 through EU8, EU16

Procedure Description:

- 1) For each EUD perform the following:
 - a) Ensure that the EUD prohibits the local storage of user data from the Red network and the use of external data storage media (EU1, EU2).
 - b) Inspect that the Inner and Outer VPN Clients on the EUD use separate private key stores (EU3).
 - c) Identify that the Inner and Outer VPN Clients on the EUD are implemented on separate IP stacks (EU4).
 - d) Verify that updates to the EUD only can be accomplished through re-provisioning (EU5).
 - e) Verify that enterprise services shall not transmit any classified data to the EUD until user authentication succeeds. (EU7).
 - f) Inspect that the EUD has full disk encrypted (EU8).
 - g) Inspect that the EUD persistently stores only unclassified configurable data (EU16).
- 2) If the EUD is remotely administrated, ensure that the EU6 is applied.

Expected Result:

For step 1, all EUDs shall be configured properly. For step 2, a remotely administrated EUD shall only be rekeyed over the VPN solution network prior to the expiration of keys.

14.4 VPN COMPONENT CONFIGURATIONS

This section contains a procedure to ensure that the configurations for all the VPN Components in the VPN solution follow the requirements given in this Capability Package.

Requirements being tested: SR4, CR1 through CR11, IR1, IR2, OR1, OR2, OR3, RA1, RA2, KM5, KM6, PF2

Procedure Description:

- 1) For each VPN component in the solution, perform the following:
 - a) Obtain the current configuration for the VPN Component.
 - b) Verify that a device certificate from a CA included in the VPN solution is listed in the configuration for authentication. Also ensure the corresponding CA signing certificate and certificate revocation information are on the VPN Component. (CR5)
 - c) Verify that the requirements CR2 through CR4, CR6 through CR11, and PF2 are configured properly.
 - d) Ensure the time of day matches the current time. This should be within a small margin of error, to be determined by the AO/DAA. (SR4)
- 2) For each Inner VPN component in the solution, use the configuration from 1a and perform the following:
 - a) Verify that the cryptographic algorithms, key sizes, and SA timeframes match what is given in Table 2 and IR1. (CR1, IR1)
 - b) Verify that IR2 has been configured.
 - c) Verify that all CA signing certificates used in the solution are from Inner tunnel CAs. (KM5)
- 3) For each Outer VPN component in the solution, use the configuration from 1a and perform the following:
 - a) Verify that the cryptographic algorithms, key sizes, and SA timeframes match what is given in Table 2 and OR1. (CR1, OR1)

- b) Verify that OR2 and OR3 have been configured.
 - c) Verify that all CA signing certificates used in the solution are from Outer tunnel CAs. (KM6)
- 4) For each device that administers a VPN Gateway in the VPN solution, verify that requirements RA1 and RA2 are configured properly.
 - 5) For each device that administers a VPN client in the VPN solution, verify that requirements RA2 and RA3 are configured properly.

Expected Result:

For Steps 1-3, all VPN Components should be configured properly based upon the requirements in Section **Error! Reference source not found.** For Steps 4 and 5, all VPN Component administration devices should be configured properly based upon the requirements of Section 10.8 of this Capability Package.

14.5 CA CONFIGURATIONS

This section contains a procedure to ensure that the configurations for all of the CAs used within the VPN solution follow the requirements given in this Capability Package.

Requirements being tested: KM1 through KM4, KM7 through KM17, SR4

Procedure Description:

- 1) Verify that requirements KM1, KM2, KM4, and KM7 are met by both CAs.
- 2) Verify that if the Inner tunnel CA is an Enterprise CA that it is operating under a CPS. If it is a Locally-run CA, verify that the Inner tunnel CA operates in accordance with both a CP and CPS. (KM3, KM11)
- 3) Verify that if the Inner tunnel CA is an Enterprise CA that it meets requirements KM9 and KM10.
- 4) Verify that the Outer tunnel CA has both a CP and CPS that it operates under. (KM3, KM11)
- 5) Verify that requirements KM12 through KM17 are met by any Locally-run CA.
- 6) Verify that the VPN Gateways were keyed in a manner consistent with KM8. Ensure that there is certificate revocation information and CA signing certificate on each VPN Gateway.
- 7) Ensure the time of day on each CA matches the current time. This should be within a small margin of error, to be determined by the AO/DAA. (SR4)

Expected Result:

For Steps 1-7, all CAs should be configured to meet the requirements being tested from Section 10.10 of this Capability Package.

14.6 VPN GATEWAY ADMINISTRATION

This section contains a procedure for ensuring that the Security Administrator can log directly into all VPN Gateways that they are administering using their credentials and that they cannot log into any VPN Gateway with default username and passwords. In addition, this test ensures that the Security Administrator can successfully administer all VPN Gateways using the method determined in the implementation of the VPN solution.

Requirements being tested: CR3, TR2, AU1, RA1

Procedure Description:

- 1) Connect the appropriate VPN Gateway administration workstation directly to each VPN Gateway using a console cable. (CR3)
 - a) Attempt to log into the VPN Gateway using the default user name and password for the VPN Gateway. Verify that a log file is created that indicates a failure to authenticate. (AU1)
 - b) Attempt to log into the VPN Gateway using a valid user name and password (this user name and password may be specifically created for testing and should be removed or changed prior to the solution going live). Verify that a log file is created that indicates a successful authentication. (AU3)
- 2) Log into each VPN Gateway using the procedures determined in the customer's specific implementation of the solution. This includes using the appropriate protocols as detailed in RA1. (TR2)
 - a) Obtain the VPN Gateway configuration from the VPN Gateway.
 - b) Create a new entry for the access control list.
 - c) Obtain again the VPN Gateway configuration.
 - d) Remove the entry created in b) from the access control list.

Expected Result:

In Step 1a, the default user name and password should be denied access to the VPN Gateway. In Step 1b, the valid user name and password should allow the tester access to the VPN Gateway.

In Step 2, the procedures should allow access to the VPN Gateway, and the change made in 2b should be found as the only difference between the Gateway configurations in 2a and 2c.

14.7 SOLUTION FUNCTIONALITY

This section contains a procedure for ensuring that end user data traverses the solution to end users on Red networks at all other sites in the solution.

Requirements being tested: TR1

Procedure Description:

- 1) Log onto the User machine on the Red network at one site in the solution (call it Site A).
- 2) Complete the following steps to establish the double tunnel to a red User machine at each other site in the solution. (TR1)
 - a) Determine the IP address for the red User machine at the other site.
 - b) From a command window on the User machine at Site A, type “ping <ip address>”. Note that in many cases, the standard timeout for the ping request will be less than the time needed to establish the double tunnel. In that case, you can change the default timeout using the following command “ping -W 7 <ip address>,” which would give a default timeout of 7 seconds. Note that if ping is disabled at a VPN Gateway, an alternate connection protocol may be used to ensure connectivity.
- 3) Repeat Steps 1 and 2 for each of the remaining sites in the solution.

Expected Result:

All ping commands will successfully receive packets of data from each site pinged. In cases where the results of the ping command are always “Request Timed Out”, that indicates a problem in the tunnels between those two sites. Additional diagnosis will be required to determine the cause of that lack of connectivity.

14.8 APPROPRIATE PACKETS TRAVERSING THE SOLUTION

This section contains a procedure for ensuring that data traversing the Gray and Black networks is protected via encryption and that no plaintext data is seen from the sites. This procedure includes verification that data traveling between the Inner and Outer VPN Gateways is limited to ESP and UDP. These tests also ensure static IP address filters on the VPN Gateways are handling packets appropriately based on IP address.

Requirements being tested: PF1, PF3 through PF5, OR2, OR3, IR2

Procedure Description:

- 1) Once the solution is configured as defined in this Capability Package, set up a packet analyzer on the black network first and then set up a packet analyzer on the gray network. Then begin capturing traffic crossing the VPN Gateways' interfaces. During the captures, regular actions from each site should be performed so that traffic simulates expected usage of the solution.
 - a) For traffic at the external interface of the Outer VPN: (PF1, OR2, OR3, PF5)
 - i) Given correct configuration, all data seen in the captured packets that originate at one of the solutions' VPN Gateways shall be encrypted. Verify that no plaintext information is visible in the data portion of these packets.
 - ii) Verify that plaintext data seen in the data portion of packets at this interface has a source address that differs from any VPN Gateway in the solution. This is either Black network traffic that does not originate from the VPN solution or from the outer VPN Gateway itself.
 - iii) Verify that multicast messages received are dropped by the Outer VPN and the event is logged.
 - b) For traffic at the external interface of the Inner VPN: (PF1)
 - i) Given correct configuration, all data seen in the captured packets that originate at one of the solutions' VPN Gateways shall be encrypted.
 - ii) Identify the packet types seen in the capture. The only traffic at this interface will be ESP or UDP.
 - iii) Using a protocol analyzer, identify that the outgoing packet for each incoming packet for packets leaving the external interface of the Inner VPN Gateway and client. If compression is used, the outgoing packet may be smaller than the incoming packet.
 - c) For traffic at the internal interface from the Gray data network of the Outer VPN: (PF1)
 - i) Given correct configuration, all data seen in the captured packets that originate at one of the solutions' VPN Gateways shall be encrypted. Using a protocol analyzer, verify that no plaintext information is visible in the data portion of these packets. (Any plaintext data seen in the data portion at this interface will indicate a problem.)
 - ii) Identify the packet types seen in the capture. The only traffic at this interface will be ESP or UDP.

- d) For traffic at the internal interface from the Gray management network of the Outer VPN: (PF3)
 - i) Given correct configuration, all data seen in the captured packets that originate at one of the solutions' VPN Gateways shall be encrypted. Using a protocol analyzer, verify that no plaintext information is visible in the data portion of these packets. (Some information such as Audit may be in plaintext here depending on your configuration. All security critical information should be encrypted.)
 - ii) Identify the packet types seen in the capture. The only traffic at this interface will be that necessary to manage the Outer VPN Gateways.
- e) For Gray management network traffic (PF4):
 - i) Identify the Gray management network traffic shall be separate from the data traffic on the Gray network.

2) When testing is complete, remove packet analyzer from the network.

Expected Result:

Any traffic on the Gray data network coming from the VPN Gateway will be encrypted and filtered so that only ESP and UDP packets are allowed provided that the VPN solution is configured properly. The traffic at the external interface of the Outer VPN Gateway that originates from this solution will also be encrypted and limited to ESP and UDP. The traffic on the Gray management network shall be separate from the Gray network. All tests above involve use of a packet analyzer and inspection of packets captured. All results are expected to be pass/fail.

14.9 APPROPRIATE PACKETS TRANSFERRING THE EUD

This section contains a procedure to ensure that only authorized network traffic occurs between the EUD and the Red network.

Requirements being tested: PF6

Procedure Description:

- 1) Once the Remote Access Architecture has been configured as defined in this Capability Package, set up a protocol analyzer on the Red Network. Then begin capturing traffic crossing the Inner VPN Gateways' interfaces. During the captures, identify that only Thin Client and remote management protocols are depicted. All other protocols are dropped.

Expected Result:

Traffic between the Red network and Inner VPN Gateways' interfaces will be restricted to only authorize communication. All results are expected to be pass/fail.

14.10 SECURITY ASSOCIATION LIFETIMES

This section contains a procedure for ensuring SAs expire as given in IR1 and OR1: IKE SA lifetime is 24 hours; ESP SA lifetime is 8 hours.

Requirements being tested: IR1, OR1

Procedure Description:

- 1) Identify the Security Parameter Index (SPI) for the established SAs for each VPN tunnel.
Note: SPIs are used as a connection identifier; these are unique identifiers of an SA (IR1, OR1).
 - a) SPIs are sent in the header of an IKE or ESP message; ESP messages contain only the recipient's SPI; IKE messages include both the sender and recipient SPIs.
 - b) Some VPN Gateways allow an administrator to query for current/active SAs. This query will provide information regarding the endpoints and the unique identifier for the SA.
- 2) Allow the network to run, as usual, for just over 8 hours.
 - a) Check that the SPIs for the ESP SAs have changed (from those seen in Step 1).
- 3) Allow the network to run, as usual, for just over 24 hours (16 hours after Step 2).
 - a) Check that the SPIs for the IKE SAs have changed (from those seen in Step 1).
 - b) Alternatively, if the connection has been inactive for some time, the connection may be terminated; this would result in the IKE SA being removed. This is also an acceptable action at lifetime expiration.

Expected Result:

Configured SA lifetimes shall be maintained. When rekeyed (or reinitialized), a new SA identifier is created; verification of a new ID indicates the SA/key lifetime is upheld. All results are expected to be pass/fail.

14.11 USE OF CERTIFICATES FROM UNTRUSTED CAS

This section contains a procedure to ensure that only certificates from trusted CAs are accepted.

Requirements being tested: KM5, KM6, AU1

Procedure Description:

- 1) Ensure that the solution is in its default setting and that the VPN connections are established when the proper certificates (see Section 6) are used to authenticate the VPN Gateways.
- 2) Install alternate certificates on the VPN Gateways, not generated by the approved CAs, and configure the solution so that one of the VPN Gateways uses this certificate for authentication. (Note that an alternate way to perform this testing is to install a certificate without its CA Signing Certificate, so that the trust anchor is not identifiable.)
 - a) Verify that an entry to the Audit log has been created due to certificate loading. (AU1)
 - b) Start the VPN connections using the new configuration.
 - c) Verify that the connection is not successful; end-to-end communication is not provided because the Gateways will fail to authenticate. Verify that failures are logged in the audit data.
 - d) Repeat this test for each VPN Gateway; only 1 VPN Gateway should offer the non-approved CA certificate per connection.
- 3) When testing is complete, remove the alternate certificates and return the configuration to its proper settings. Verify that an entry to the Audit log has been created due to certificate deletion. (AU1)

Expected Result:

Authentication will not occur when the VPN Gateways cannot identify the trust anchor of the certificates, provided the solution is configured correctly. All results are expected to be pass/fail.

14.12 USE OF REVOKED CERTIFICATES

This section contains a procedure to ensure that only valid certificates are accepted. This section focuses on certificates that have been revoked (and are therefore invalid) and does not include all types of validity testing.

Requirements being tested: CR5, CR7, KM14, AU1

Procedure Description:

- 1) Ensure that the solution is in its default setting and that the VPN connections are established when the proper, valid certificates (see Section 6) are used to authenticate the VPN Gateways.

- 2) Revoke a certificate for one of the VPN Gateways (or install an alternate revoked certificate on one of the VPN Gateways), and ensure the solution is configured so that this revoked certificate will be used for authentication.
 - a) If applicable, verify that an entry to the Audit log has been created due to certificate loading. (AU1)
 - b) Ensure the VPN Gateways contain the latest certificate revocation information to include the revoked certificate to be used for authentication. (KM14)
 - c) Start the VPN connection.
 - d) Verify that the connection is not successful; end-to-end communication is not provided because the Gateways will fail to authenticate the revoked certificate. Verify that failures are logged in the audit data. (CR5, CR7, KM14, AU1)
 - e) Repeat this test for each VPN Gateway; only one VPN Gateway should offer the revoked certificate per connection.
- 3) When testing is complete, remove the revoked certificates and return the configuration to its proper settings. Verify that an entry to the Audit log has been created due to certificate deletion. (AU1)

Expected Result:

Authentication will not occur when the VPN Gateways cannot verify the validity of the certificates, provided the solution is configured correctly. All results are expected to be pass/fail.

14.13 CONFIGURATION CHANGE DETECTION

This section contains a procedure to ensure that changes made to any of the VPN Gateway configurations are detected by the Configuration Change Detection tool.

Requirements being tested: CM1, CM2, AU1

Procedure Description:

- 1) The following steps shall be done for each of the VPN Gateways within the solution.
 - a) Log into the VPN Gateway.
 - b) Compare the current version of the VPN Gateway configuration with the stored baseline and ensure that the current version matches the stored configuration. (CM1)
 - c) Make a change to the configuration, preferably something that is not fundamental to the security of the VPN solution.

- d) Look in the audit log to determine if a log entry has been generated about the configuration change and that the changes from c) are recorded. (AU1, CM2)

Expected Result:

The administrator will validate that the baseline configuration was stored in Step 1b. In Step 1d, there should be a log entry created for the configuration change in the audit log including the actual configuration change.

14.14 AUDIT

This section contains procedures for ensuring that audit events are detected, that the proper information is logged for each event, and that there is a procedure detailed in the CPS documentation for auditing each CA device.

Requirements being tested: AU1, AU2, AU3, CR10

Procedure Description:

- 1) Examples for testing the ability of each VPN Gateway to audit and log audit events specified in AU1 are given below. Additional tests for the events in AU1 are included in appropriate tests in other areas within this testing section. Verify that for each event logged, the applicable data regarding the event is recorded for the log entry in accordance with AU3.
 - a) All actions performed by a user with super privileges (auditor, administrator, etc.) and any escalation of user privileges.
 - i) Log in as an administrator to the VPN Gateway.
 - ii) Perform a variety of administrator actions on the VPN Gateway.
 - iii) Verify that a log entry was created for each action taken in Step ii that required super-user privileges.
 - iv) Revert back to the baseline configuration, eliminating the changes made in Step ii.
 - v) Repeat the above with the Auditor role.
 - b) Changes to time
 - i) Log in as an administrator to the VPN Gateway.
 - ii) Modify the system time on the VPN Gateway by at least 1 hour.
 - iii) Verify that a log entry was created due to the change in system time.
 - iv) Revert the system time back to the accurate time of day.

- c) All built-in self-test results, which may indicate failures in cryptographic functionality
 - i) Completely power down the VPN Gateway.
 - ii) Power the VPN Gateway back up so that the automatic self-tests are run.
 - iii) Verify that a log entry was created due to running the self-tests.
- 2) Verify that the VPN Gateway's loopback address is used as the source address for all audit log entries. (CR10)
- 3) Verify that there is a procedure detailed in the CPS documentation for auditing each CA device within the solution. (AU2).

Expected Result:

For Step 1, all occurrences of auditable events given in AU1 should generate an entry in the audit log including all the information given in AU3. For Step 2, the source address should be the VPN Gateway's loopback address. For Step 3, there should be a procedure for auditing the CA devices in the solution that is outlined in the CPS document.

14.15 IMPLEMENTATION OF GUIDANCE

This section ensures that there are procedures in place and/or that procedures were followed regarding the procurement of products and use of the VPN solution. It also ensures that the personnel in place to manage and administer this solution follow the guidelines given in the Capability Package.

Requirements being tested: GD1 through GD17

Procedure Description:

- 1) Verify that the procedures given in GD1, GD2, GD3, GD7, GD8, GD9, GD10, GD11, GD12, and GD13 were/are followed and/or are currently in place.
- 2) Verify that the solution owner understands that he/she shall allow and fully cooperate with an NSA-ordered IA compliance audit of this solution implementation. (GD4)
- 3) Verify that the solution owner and AO/DAA are aware that a compliance audit will be conducted every 3 years. (GD5)
- 4) Verify that the solution owner and AO/DAA are aware that when new versions of the VPN Capability Package are published by NSA, they will have 6 months to move into compliance with this new version. (GD5)

- 5) Verify that the solution owner and AO/DAA are aware that they shall provide updated solution information to NSA on a yearly basis. (GD6)
- 6) Verify that the personnel requirements given in GD14 through GD17 are met by the personnel supporting this implementation of the VPN solution.

Expected Result:

For 1-6, all of these procedures have been followed or are in place.

APPENDIX A. GLOSSARY OF TERMS

Accreditation – The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls. (NIST 800-37)

Assurance – A measure of confidence that the security features and architecture of an AIS accurately mediate and enforce the security policy. Certification by designated technical personnel of the extent to which design and implementation of the system meet specified technical requirement for achieving adequate data security.

Audit – The activity of monitoring the operation of a product from within the product. It includes monitoring of a product for a set of pre-determined events. Each audit event may indicate rogue behavior, or a condition that is detrimental to security, or provide necessary forensics to identify the source of rogue behavior.

Audit log – A chronological record of the audit events that have been deemed critical to security. The audit log can be used to identify potentially malicious activity that may further identify the source of an attack, as well as potential vulnerabilities where additional countermeasures or corrective action are required.

Availability – Assurance that the system and its associated assets are accessible and protected against denial or service attacks, as well as available when the user needs them and in the form needed by the user.

Black box testing – Testing the functionality of a component of the solution, such that testing is limited to the subset of functionality that is available from the external interfaces of the box during its normal operational configuration without any additional privileges (such as given to the Security Administrator or Auditor).

Capability Package – The set of guidance provided by NSA that describes recommended approaches to composing COTS components to protect classified information for a particular class of security problem. This package will point to potential products that can be used as part of this solution.

Certification – The technical evaluation of a system's security features, made as part of and in support of the approval/accreditation process that establishes the extent to which a particular computer system's design and implementation meet a set of specified security requirements.

Certification and Accreditation (C&A) – A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating

as intended, and producing the desired outcome with respect to meeting the security requirements for the system. In conjunction with the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls. (NIST 800-37).

Certificate Authority (CA) – An authority trusted by one or more users to create and assign certificates. [ISO9594-8]

Certificate Policy (CP) – A named set of rules that indicate the applicability of a certificate to a particular community and/or class of application with common security requirements. For example, a particular CP might indicate applicability of a type of certificate to the authentication of parties engaging in business-to-business transactions for the trading of goods or services within a given price range. [RFC 3647]

Committee on National Security Systems Policy No. 15 (CNSSP-15) – Policy specifies which public standards may be used for cryptographic protocol and algorithm interoperability to protect National Security Systems (NSS).

Confidentiality – Assurance that the data stored in, processed by, or transmitted by the system are protected against unauthorized disclosure and confidence in that only the appropriate set of individuals or organizations would be provided the information.

Designated Approving Authority (DAA) – The official with the authority to formally assume responsibility for operating a system at an acceptable level of risk, synonymous with designating accrediting authority and delegated accrediting authority. [CNSSI 4009]

End User Device (EUD) – The component which terminates both IPsec VPN tunnels in the Remote Access Architecture.

External Interface – The interface on a VPN Gateway that connects to the outer network (i.e., the Gray network on the Inner VPN Gateway or the Black network on the Outer VPN Gateway).

Federal Information Processing Standards (FIPS) – A set of standards that describe the handling and processing of information within governmental agencies.

Gray Box testing – The ability to test functionality within a component of the solution, such that full management privileges are granted (i.e., knowing passwords for security administrator and Auditor and access to the capabilities associated with those privileges). In addition, the use of any and all testing equipment and/or testing software used inside and outside the developed solution is available.

Internal Interface – The interface on a VPN Gateway that connects to the inner network (i.e., the Gray network on the Outer VPN Gateway or the Red network on the Inner VPN Gateway).

May – This word means that an item is truly optional. Some customers may choose to include the item in their VPN solution while others may not.

Protection Profile – A document used as part of the certification process according to the Common Criteria. As the generic form of a security target, it is typically created by a user or user community and provides an implementation independent specification of information assurance security requirements.

Public Key Infrastructure (PKI) – Framework established to issue, maintain, and revoke public key certificates.

Shall – This word means that the definition is an absolute requirement of this Capability Package.

Should – This word means that there may exist valid reasons in particular circumstances to ignore a particular requirement in this Capability Package, but the full implications must be understood and carefully weighed before choosing a different course.

VPN Client – A VPN application installed on the EUD in the Remote Access Architecture.

VPN Component – The term used to refer to VPN Gateways and VPN Clients.

VPN Gateway – The VPN device physically located within the VPN infrastructure.

VPN Infrastructure – Physically protected in secure facility and includes Inner and Outer VPN Gateways and may also include Certificate Authorities and Administrative devices.

APPENDIX B. ACRONYMS

ACL	Access Control List
AES	Advanced Encryption Standard
AO	Authorizing Official
ARP	Address Resolution Protocol
BFD	Bidirectional Forwarding Detection
C&A	Certification and Accreditation
CA	Certificate Authority
CAA	Certificate Authority Administrator
CCI	Controlled Cryptographic Item
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
CNSSP	Committee on National Security Systems Protocol
COTS	Commercial Off-the-Shelf
CP	Certificate Policy
CPS	Certification Practice Statement
CSfC	Commercial Solutions for Classified
DAA	Designated Approving Authority
DDoS	Distributed Denial of Service
DH	Diffie Hellman
DISA	Defense Information Systems Agency
DNS	Domain Name System
DoS	Denial of Service
DSA	Digital Signature Algorithm
ECDH	Elliptic Curve Diffie Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
ESP	Encapsulating Security Payload
EUD	End User Device
FIPS	Federal Information Processing Standards
GOTS	Government Off-the-Shelf
GRE	Generic Routing Encapsulation
HAIPe	High Assurance Internet Protocol Encryption
IAD	Information Assurance Directorate
IAVA	Information Assurance Vulnerability Alerts
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IKE	Internet Key Exchange

IP	Internet Protocol
IPS	Intrusion Prevention System
IPsec	Internet Protocol Security
MLD	Multicast Listener Discovery
MPLS	Multi-Protocol Label Switching
MTU	Maximum Transmission Unit
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSS	National Security Systems
NTP	Network Time Protocol
OID	Object Identifier
OS	Operating System
OSPF	Open Shortest Path First
PKI	Public Key Infrastructure
PMTU	Path Maximum Transmission Unit
RFC	Request for Comment
RSA	Rivest Shamir Adelman algorithm
S3	Secure sharing suite
SA	Security Association
SHA	Secure Hash Algorithm
SIPRNet	Secret Internet Protocol Router Network
SP	Service Packs
SSH	Secure Shell
T&E	Test and Evaluation
TLS	Transport Layer Security
VM	Virtual Machine
VPN	Virtual Private Network

APPENDIX C. REFERENCES

CNSSI 4009	<i>CNSSI 4009, National Information Assurance (IA) Glossary Committee for National Security Systems www.cnss.gov/Assets/pdf/cnssi_4009.pdf</i>	April 2010
CNSSP 15	<i>CNSS Policy (CNSSP) Number 15, National Information Assurance Policy on the Use of Public Standards for the Secure Sharing of Information Among National Security Systems Committee for National Security Systems</i>	March 2010
FIPS 140	<i>Federal Information Processing Standard 140, Security Requirements For Cryptographic Modules National Institute for Standards and Technology FIPS Publication http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf</i>	May 2001
FIPS 180	<i>Federal Information Processing Standard 180-4, Secure Hash Standard (SHS)</i>	March 2012
FIPS 186	<i>Federal Information Processing Standard 186-3, Digital Signature Standard (DSS), (Revision of FIPS 186-2, June 2000)</i>	June 2009
FIPS 197	<i>Federal Information Processing Standard 197, Advanced Encryption Standard (AES)</i>	November 2001
FIPS 201	<i>Federal Information Processing Standard 201, Personal Identity Verification (PIV) of Federal Employees and Contractors National Institute for Standards and Technology FIPS Publication http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf</i>	March 2006
IPsec VPN Client PP	<i>IPsec VPN Client Protection Profile. www.niap.ccevs.org/pp</i>	January 2012
NSA Suite B	<i>NSA Guidance on Suite B Cryptography [including the Secure Sharing Suite (S3)]. http://www.nsa.gov/ia/programs/ suiteb_cryptography/index.shtml</i>	November 2010
RFC 2409	<i>IETF RFC 2409 The Internet Key Exchange (IKE). D. Harkins and D. Carrel.</i>	November 1998
RFC 3647	<i>IETF RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework Internet Engineering Task Force http://www.ietf.org/rfc/rfc3647.txt</i>	November 2003

RFC 4252	<i>IETF RFC 4252 The Secure Shell (SSH) Authentication Protocol.</i> T. Ylonen and C. Lonvick.	January 2006
RFC 4253	<i>IETF RFC 4253 The Secure Shell (SSH) Transport Layer Protocol.</i> T. Ylonen and C. Lonvick.	January 2006
RFC 4254	<i>IETF RFC 4254 The Secure Shell (SSH) Connection Protocol.</i> T. Ylonen and C. Lonvick.	January 2006
RFC 4302	<i>IETF RFC 4302 IP Authentication Header.</i> S. Kent	December 2005
RFC 4303	<i>IETF RFC 4303 IP Encapsulating Security Payload.</i> S. Kent	December 2005
RFC 4307	<i>IETF RFC 4307 Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2).</i> J. Schiller	December 2005
RFC 4308	<i>IETF RFC 4308 Cryptographic Suites for IPsec.</i> P. Hoffman	December 2005
RFC 5246	<i>IETF RFC 5246 The Transport Layer Security (TLS) Protocol Version 1.2.</i> T. Dierks and E. Rescorla.	August 2008
RFC 5996	<i>IETF RFC 5996 Internet Key Exchange Protocol Version 2 (IKEv2).</i> C. Kaufman, et. al.	September 2010
RFC 6379	<i>IETF RFC 6379 Suite B Cryptographic Suites for IPsec.</i> L. Law and J. Solinas.	October 2011
RFC 6460	<i>IETF RFC 6460 Suite B Profile for Transport Layer Security (TLS).</i> M. Salter, et.al.	January 2012
SP 800-56A	<i>NIST Special Publication 800-56A, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography.</i> E. Barker, D. Johnson, and M. Smid	March 2007
SP 800-56B	<i>NIST Special Publication 800-56B, Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography.</i> E. Barker, et. al.	August 2009
SP 800-56C	<i>NIST Special Publication 800-56C, Recommendation for Key Derivation through Extraction-then-Expansion.</i> L. Chen.	November 2011
SP 800-131A	<i>NIST Special Publication 800-131A, Recommendation for Transitioning of Cryptographic Algorithms and Key Lengths.</i> E. Barker.	January 2011

SP 800-147 *NIST Special Publication 800-147, BIOS Protection Guidelines.* D. April 2011
Cooper, et. al.

APPENDIX D. EXAMPLE IAD APPROVAL LETTER FOR VPN CAPABILITY PACKAGE SOLUTIONS

A sample IAD approval letter for VPN Capability Package solutions will be included in a future version of this Capability Package.

APPENDIX E. END USER DEVICE IMPLEMENTATION NOTES

In the Remote Access architecture, the End User Device (EUD) contains the Inner and Outer VPN Clients as well as the Thin Client application, all of which work together to provide the user with remote access to a classified network. Although this Capability Package levies several requirements on the EUD, it does not specify how to implement the EUD in order to meet those requirements. System developers have flexibility in choosing how to implement their EUDs, as long as they comply with this Capability Package's requirements.

EXAMPLE EUD IMPLEMENTATION APPROACHES

This appendix lists example design choices that system developers can make when implementing their EUDs, and is intended for illustrative purposes only. Following one of the designs in this appendix is **not** a requirement for compliance with this Capability Package. Conversely, following one of the designs in this appendix does **not** by itself guarantee that the resulting implementation necessarily complies with the requirements of this Capability Package.

Since an EUD physically connects directly to the Black network, there is no physical Gray or Red network on its side of the VPN connection. However, data flows within the EUD can be considered Red, Gray, or Black based on the number of layers of encryption that have been applied to the data.

EXAMPLE 1: TYPE 2 VIRTUALIZATION

The first example for implementing the EUD is to use virtualization to run the Inner and Outer VPN Clients on separate operating systems (OSes). Since each OS implements its own IP stack, the design meets requirement EU4. Running the Inner and Outer VPN Clients on separate OSes also prevents them from using the same private key store, meeting requirement EU3.

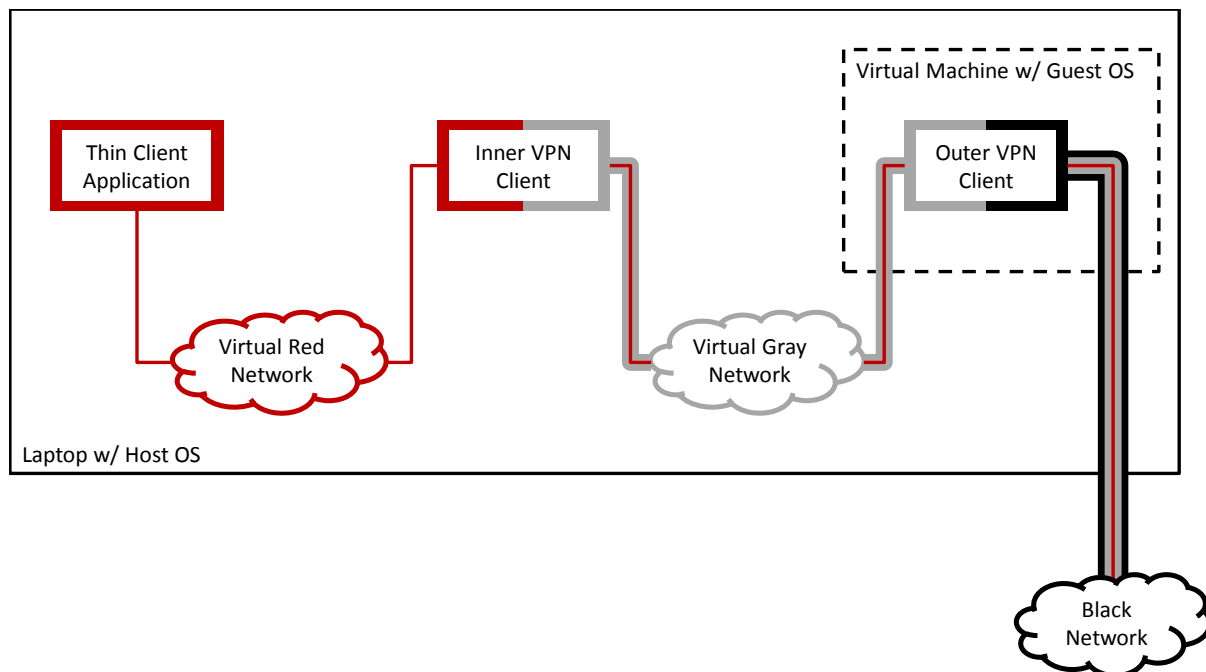


Figure 6. Example EUD Implementation using Type 2 Virtualization

In this example, illustrated in Figure 6, the EUD is an ordinary laptop running a virtual machine (VM) on a Type 2 (hosted) hypervisor. The Outer VPN Client runs within the virtual machine on top of the guest OS. The Inner VPN Client and the Thin Client Application both run outside of the virtual machine, on top of the host OS.

The laptop's physical network interface is bridged directly to the virtual machine, preventing applications (other than the virtual machine itself) from directly communicating over the Black network. The virtual machine software creates a virtual network between the host and guest OSes which acts as the Gray network within the EUD; the host and guest OSes each have a virtual network interface to this network. The Inner VPN Client also creates an additional virtual network interface on the host OS, which the Thin Client Application will connect to; this virtual network acts as the Red network within the EUD.

The host OS is configured to only allow the Inner VPN Client to connect to the virtual Gray network interface. The host OS's routing table forces all other network traffic through the virtual Red network interface. The Inner VPN Client encrypts all data sent through this interface and forwards it to the virtual Gray network into the guest OS, where the Outer VPN Client encrypts it a second time before sending it out the bridged physical interface to the Black network. Traffic arriving at the EUD follows the reverse path to be decrypted twice before being provided to the Thin Client Application.

The guest OS can implement packet filtering on both its Gray and Black network interfaces. The packet filter on the Gray interface would block all traffic except IKE, ESP, and remote

management protocols. The packet filter on the Black interface would block all traffic except IKE, ESP, and protocols such as DHCP or DNS needed to join the Black network and connect to the Outer VPN Gateway.

EXAMPLE 2: TYPE 1 VIRTUALIZATION

The second example for implementing the EUD also involves the use of virtualization to run the Inner and Outer VPN Clients on separate OSes. This example takes the approach further by using a Type 1 (native) hypervisor to run the Outer VPN Client, Inner VPN Client, and Thin Client Application each in their own virtual machines, as shown in Figure.

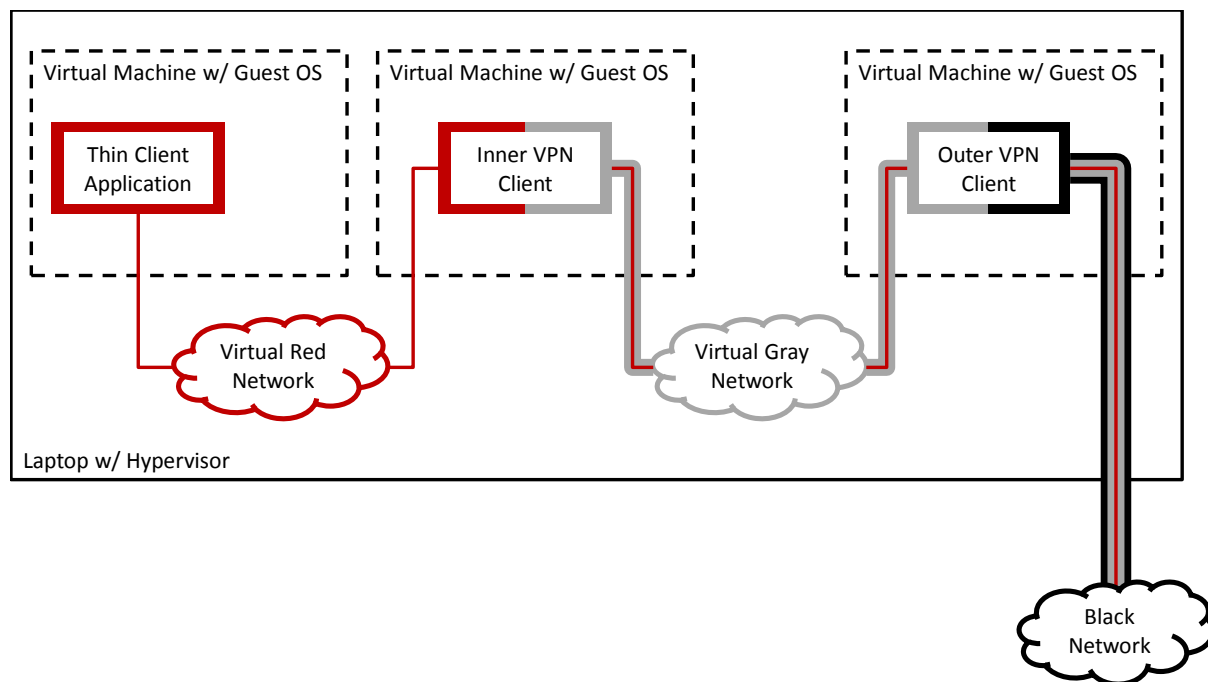


Figure 7. Example EUD Implementation using Type 1 Virtualization

As in the first example, the laptop's physical network interface is bridged directly to the virtual machine that contains the Outer VPN Client. The hypervisor creates two virtual networks: a virtual Gray network between the VM for the Outer VPN Client and the VM for the Inner VPN Client, and a virtual Red network between the VM for the Inner VPN Client and the VM for the Thin Client Application. The virtual network configuration forces all traffic leaving the Thin Client Application to go through both the Inner and Outer VPN Clients before passing over the Black network.

The guest OSes for the Inner and Outer VPN Clients could implement packet filtering for each of their interfaces, or the packet filtering could be performed by the hypervisor. Packet filters for the virtual Red network would block all traffic except for Thin Client and remote management protocols. Packet filters for the virtual Gray network would block all traffic except for IKE, ESP,

and remote management protocols. Packet filters for the Black network would block all traffic except IKE, ESP, and protocols such as DHCP or DNS needed to join the Black network and connect to the Outer VPN Gateway.

EXAMPLE 3: EXTERNAL OUTER IPSEC CLIENT DEVICE

The third example for implementing the EUD takes a different approach to separating the Inner and Outer VPN Clients: moving the Outer VPN Client to a peripheral or other device with a direct, physical connection to the laptop hosting the Inner VPN Client. This external device could take the form of, for example, a USB network adaptor with an integrated IPsec client, as shown in Figure. With this implementation, the EUD consists of the laptop, the IPsec device, and the physical connections between them.

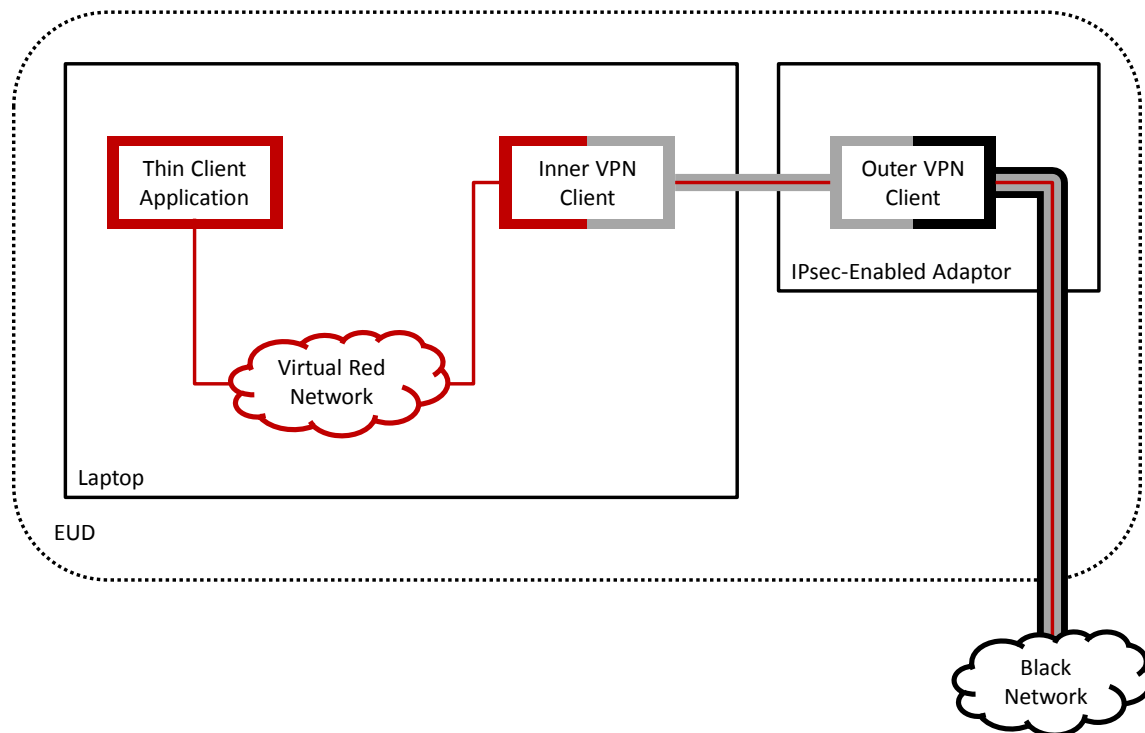


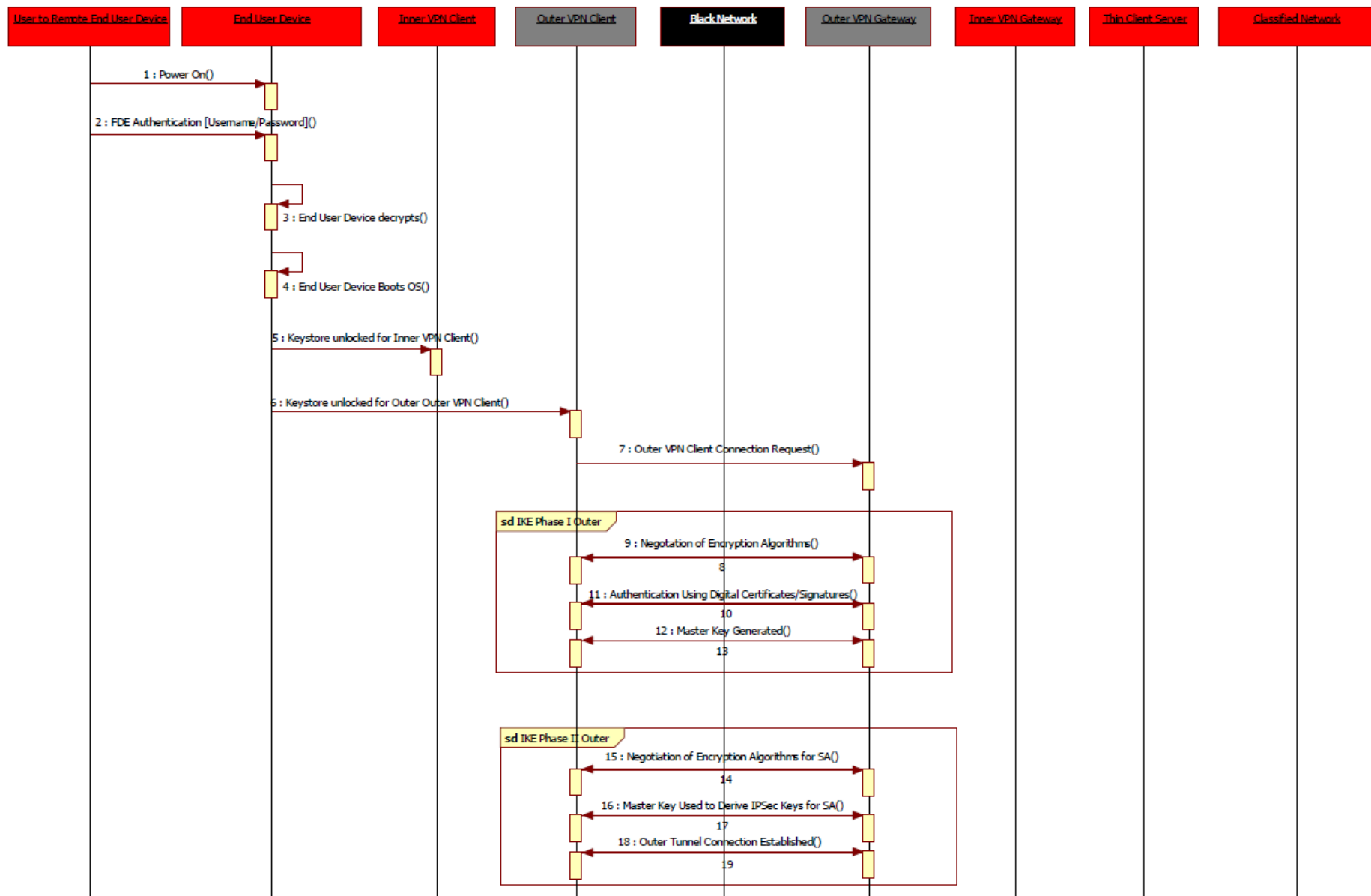
Figure 8. Example EUD Implementation using an External Outer IPsec Client Device

In this example, the physical connection between the laptop and the IPsec device serves the same role as a Gray network. The Inner VPN Client running on the laptop creates a virtual network interface that serves as the Red network, which the Thin Client Application connects to. The OS's routing table forces all network traffic through the virtual Red network interface. The Inner VPN Client encrypts all data sent through this interface and forwards it through the physical Gray connection to the external device, where the Outer VPN Client encrypts it a second time before sending it out to the Black network.

The OS on the laptop could implement packet filtering on the Gray network interface provided by the driver for the external device. The packet filter for the Gray network would block all traffic except for IKE, ESP, and remote management protocols.

UML SEQUENCE DIAGRAM FOR EUD TUNNEL ESTABLISHMENT

The Unified Modeling Language (UML) sequence diagram below illustrates one possible sequence of events an EUD might take from power-up to the user accessing classified data through the solution. The diagram shows how the parts of the EUD interact with components in the infrastructure site to establish the tunnels and authenticate the user.



Continued Below

